정보전 대응을 위한 전자적 증거포착 메커니즘 설계[1)]

박명찬* · 이종섭* · 최용락**

목 차

1. 서론

정보화가 급속도로 진전되고 인터넷을 통한 다양한 서비스가 확대됨에 따라 모든 비즈니스 커뮤니케이션이 정보망을 통해 서비스를 제공하고 있다. 이러한 발전은 정보화 사회에 순기능과 역기능

* 대전대학교 컴퓨터공학 박사과정,
** 대전대학교 컴퓨터공학 전공교수

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

이라는 두 가지 효과를 가져왔다. 먼저, 대부분의 업무에 있어 간편하고 편리하게 이용할 수 있는 편의성을 제공해주는 순기능이 있다면, 불법적인 해킹이나 바이러스에 의한 침해사고의 역기능이 생겨났다. 21세기 들어 정보화의 역기능은 단순한 침해의 성격에서 벗어나 하나의 사이버테러로써 범국가적으로 이루어지고 있으며, 사이버테러에 대한 피해는 전 세계적으로 확대되고 있다. 최근 많은 연구기관과 보안업체에서는 네트워크 상에서 발생되는 각종 사이버테러로부터 시스템 및 정보자산을 보호하기 위하여 다양한 보안시스템들을 개발하여 운용하고 있다.

그러나 현재 사용 중인 각종 보안 시스템들은 수동적인 침입 방어 시스템으로 공격자의 침입시도 자체를 제한하는 것이 아니라 침입이 시도된 후 공격자를 막기 위한 것으로 동일한 공격자의 재공격을 방지하는데 한계가 있다 또한, 침해사고 발생 시 시스템에 자동 저장되는 로그파일을 이용하여 사고를 분석하고 공격의 증거자료로 사용하는데 있어 로그파일에 대한 신뢰성에 대한 문제가 제기된다. 현재 대부분의 시스템의 경우, 관리자가 모든 시스템 파일에 대하여 수정 및 삭제가 가능하다. 즉, 공격자의 최우선 공격 형태는 해당 시스템의 관리자 권한의 획득이므로 피해 시스템에 남아있는 로그파일에 대한 신뢰성을 보장할 수 없다. 그리고 동일한 공격이 전체 네트워크의 서로 다른 부분에서 인식되는 정보와 전체 네트워크 차원에서 해당 데이터를 상호 결합하는 기능이 부족하여 공격자에 대한 대응에 있어서도 각 도메인 간의 협력이 없는 상태이다. 그러므로 동일한 공격이 서로 다른 네트워크에 가해졌을 때 공격에 대한 정보가 없는 곳에서는 공격을 탐지 할 수 없는 문제점을 내포하고 있다[1,2].

따라서 불법적인 침해사고를 일으키는 공격자에 대해 침입시도 자체를 제한하는 소극적인 대응을 넘어서, 우회공격이나 신분위장

공격 등에도 대응할 수 있도록 공격자의 위치를 추적하여 대응하는 능동적인 대응 기술이 필요하다. 또한, 피해 시스템에 남아있는 로그정보에 대한 신뢰성 회복을 위한 무결성 서비스 제공 방안이 필요하며, 시스템 상호간 협력할 수 있는 체제가 필요하다.

1970년대부터 미국을 비롯한 선진국에서는 중요 정보처리를 위한 컴퓨터 시스템의 필요성을 인식하고, 신뢰성을 평가할 수 있는 기준을 제정하고, 보안 운영체제를 연구하여 안전하고 신뢰성 있는 컴퓨터 시스템 개발에 많은 투자를 해 왔다. 1980년대 이후부터는 OS의 커널 수준에 안전한 운영체제를 탑재한 컴퓨터 시스템을 보급하기 시작했다. 미국의 경우, 신뢰성 컴퓨터 평가 기준(TCSEC: Trusted Computer System Evaluation Criteria)B1급 이상의 컴퓨터 시스템에서는 안전한 OS의 구현은 대부분 보안 커널(Security Kernel)로 구현하고 있으며, B2급 이상의 평가를 받은 컴퓨터 시스템에 대해서는 해외로 수출을 금지하고 있다[1].

보안 커널은 컴퓨터 운영체제상에 내재된 보안상의 결함으로 인하여 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제에 보안 기능이 통합된 보안 모듈을 올린 운영체제이다. 컴퓨터 시스템 자체를 통제하는 운영체제에 보안기능을 부여하였기 때문에 다른 보안 애플리케이션 보다 강력한 보안기능을 제공하고 운영체제 및 애플리케이션의 취약점으로 인한 보안상 결함을 원천적으로 차단한다.

본 논문에서는 미래의 정보전 환경에 대응하기 위한 국내의 대응 기술을 소개하고, 보안침해사고에 대한 기술적 증거확보와 역추적 및 재해복구를 효과적으로 수행할 수 있는 컴퓨터 포렌식스 기술을 적용한 증거포착 메커니즘을 제안한다. 또한, 증거포착 메커니즘을 통하여 사이버 공간을 침투하는 해커들의 다양한 시도 및 침투 증거를 포착하고 이들의 침투경로에 대한 추적과 시스템을 보호할 수

있는 가상 유인 메커니즘을 제안한다.

2. 관련연구

2.1 정보전

고도화된 사회 구조 속에서 정보통신에 대한 의존도는 나날이 증대되고 세계 각국은 정보화된 미래사회를 위해 국가정보통신 기반구조(NII: National Information Infrastructure)구축에 박차를 가하고 있다. 국가정보통신기반구조란 정보통신기술을 활용해서 정보유통과 관련된 설비를 관리, 통제하기 위한 정보시스템 및 정보통신망을 의미한다. 즉, 군사적 목적의 국방정보통신, 전력이나 가스를 저장 수송하는 에너지, 항공운항 등 교통, 금융 등 우리 생활중심을 구축하고 있는 기반구조를 의미한다[6,7].

정보전은 적들로부터 자신의 중요 정보자원 및 정보시스템에 대해 보호하려는 측면이 강하다. 또, 적의 중요 정보자원 및 시스템에서 우위를 차지하려는 행동으로 정보 파괴, 정보흐름 변경, 정보에 대한 신뢰성 감소, 서비스 부인공격 등이 포함된다. 정보전 전문가 Winn Schwartau는 "정보전은 상대방의 위협에 대응하여 자신의 정보자산을 보호하기 위한 기술이며 자신의 정보통신기반구조에 대한 비밀을 보장함과 동시에 상대방의 비밀을 절취하는 기술이다. 정보전은 정보를 소유하고 있는 자로부터 정보를 얻어내는 기술이며 상대방이 자신의 기술과 정보를 사용하지 못하도록 하는 것이다."고 정의하였다. 또한 미 합참은 "정보 우위를 달성하기 위하여 아군의 정보, 정보 프로세스, 정보시스템, 컴퓨터 네트워크를 보호하고, 적군의 정보, 정보 프로세스, 정보시스템, 컴퓨터 네트워크를

공격하는 일체의 행위"라 정의한바 있다[8-10].

근래에 정보전은 국가 안보 및 국가 경제 보호차원에서 새롭고 중요한 분야로 떠오르고 있다. 전력시스템, 금융시스템, 전화망, 영공관리시스템 같은 민감하지만 비밀로 분류되지 않은 데이터에 대한 공격이 초래할 대혼란을 우려해서다. 새로운 공격에 대한 결과는 아직 알려지지 않았지만 종래의 전쟁과 비교하여 볼 때 저렴한 개발비용, 실행의 용이성, 감시/감지/추적의 어려움, 익명성 보장, 실행시 미치는 거대한 파급효과 등 그 영향력은 핵전쟁의 파괴력에 버금갈 것으로 예상된다. 특히 정보사용에 대한 폭발적 요구가 증가하는 반면, 정보전에 대한 확실한 처벌법이나 국제법이 없으며, 정보전 공격에 대한 보호대책이 미비하기에 문제의 심각성은 더욱 크다. 일반적인 정보전의 속성은 익명성으로 인한 공격행위 용이, 침입하려는 목표시스템이 다수 존재, 지역적, 공간적, 정치적 경계 부재, 저투자비용에 비해 고도의 기술 획득용이 등을 들 수 있다.

21세기 정보통신고도화사회에서 정보전의 위협을 극복하고 국가적 보안체계 확립을 구축하는 일은 시급하다. 정보전은 산업사회를 거쳐 고도 정보화 사회로 진입하면서 나타나는 새로운 형태의 위협이며 그 피해는 개인 프라이버시 침해, 국가경제위기, 사회혼란, 국가안보 침해까지 다양한 형태로 나타나기 때문이다. 정보전에 대비하여 관련 법·제도 정비, 기술개발, 인력양성, 정보보호 산업육성 등 다각도의 구체적인 대응이 필요한 때이다.

2.2 대응기술

정부, 군, 산업 조직의 대규모 상호 연결된 통신 정보시스템에 대한 의존도가 증가하였다. 주요 시스템의 기밀성, 무결성, 또는 가용

성에 손실이 오는 경우 경제적, 국가적으로 심각한 영향을 초래한다. 그러므로 중요 시스템에 대한 침입을 정확하게 탐지하고 재빨리 대응하는 기술이 요구된다. 표 1은 정보전에 대한 대응기술이다[2].

<표 1> 대응기술

분류	대응 기술
보호(Protect)	■ 암호, 침입차단시스템, 인증
탐지(Detect)	■ 악의적 소프트웨어 ■ 네트워크 현황/토폴로지 ■ 전조(Precursors), 침입 ■ 자원오용, 자료 시각화 ■ 자료 상관성/집합
반응(React)	■ 대응, 복구 및 재구성
공격(Attacks)	■ 컴퓨터 바이러스, 웜 ■ 트로이목마, 트랩도어, 침입자 유인

컴퓨터 통신망의 시스템 자원에 대한 파괴, 악성 바이러스의 침투 또는 비정상적인 동작이 탐지된다면 먼저, 감지된 증상들이 특정 자원의 파괴, 해킹, 트로이 목마나 바이러스 등의 악성 소프트웨어 공격, 또는 하드웨어 장비와 소프트웨어의 오동작인지 그 원인을 알기 위하여 컴퓨터 시스템과 정보통신기기에 남아 있는 여러 가지의 전자적 흔적들을 진단해야 할 것이다.

정보보안 침해사고로부터 전자적인 현상에 의하여 과학적으로 그 원인을 진단하고 분석하여 법의학적인 증거를 제시하고 대응할 수 있는 기법이 컴퓨터 포렌식스(Computer Forensics)이다[2,11,12]. 미

국을 중심으로 한 기술 선진국들은 정보시스템에 대한 보안침해사고에 대하여 디지털 전자적 증거를 분석하고 대응하는 기술들을 개발하고 있다. 정보전에서 다양한 전자적 침해사고에 대하여 현장을 검증하고 사건의 원인과 공격루트를 밝혀내어 법적으로 보장되는 정확한 증거를 확보하는 것을 출발점으로 하여 진정한 정보의 주인이 될 수 있다. 즉, 자국의 컴퓨터 포렌식스 기술이 확보되지 않는다면 국내외에서 일어나는 모든 보안침해사고에 대하여 국가 자존적 해석이나 사실증명이 불가능하고 외국에 의뢰하여 결과를 통보받아야 하는 안타까운 현실을 초래할 수밖에 없을 것이다.

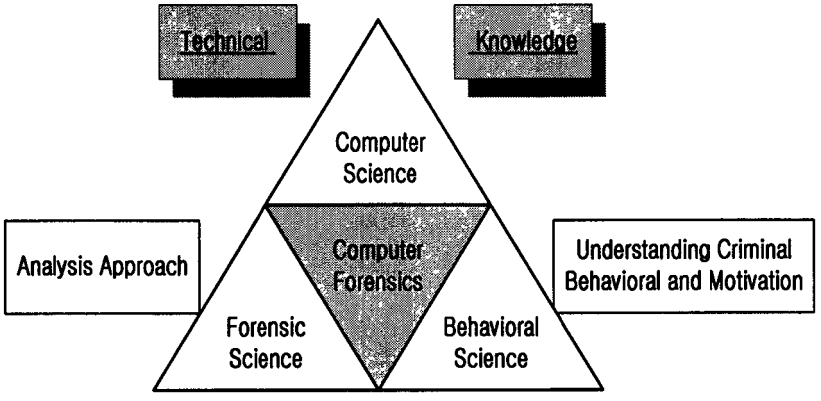
따라서, 우리나라도 정보시대의 산업기반시설 동맥이 되는 주요 설비의 보호, 정보기술 강국으로써의 자국 정보보호 및 상대국 정보의 획득, 첨단 전자무기체계 개발을 통한 공격 및 보호 기술에 대한 개발 등이 필요하다. 컴퓨터 포렌식스는 정보시스템 자원에 대한 각종 보안침해사고에 대하여 증거의 확보, 원인의 분석, 절차에 따른 단계적 대응 및 문제점 개선을 통한 향후 대응책 보완수립 등 정보전에 대비하여 반드시 필요한 원천 기술이다.

3. 컴퓨터 포렌식스

불과 2-3년 사이에 인터넷 망을 통한 사이버테러가 범국가적으로 이루어지고 있고, 인터넷의 활용성 증가와 함께 컴퓨터 범죄의 수법 또한 지능적이고 다양화되어 가고 있다. 따라서 미국을 중심으로 한, 기술 선진국들은 보안 침해사고에 대하여 디지털 전자적 증거분석 및 대응기술 개발에 집중하고 있다. 이러한 기술들은 다양한 보안침해사고의 법의학적 분석 및 복구는 물론 안전한 비즈니스

커뮤니케이션의 제도적 정착을 위하여 금융권 및 사이버 범죄수사 관련 기관의 중요한 관심사항이 되고 있다.

네트워크 환경으로부터 디지털 컨텐츠의 모든 접근행위에 대하여 전자적 증거물을 수집분석 및 역추적 등의 절차를 수행하고 법적 증거물 제시와 적절한 대응조치를 할 수 있도록 새롭게 출현한 기술이 컴퓨터 포렌식스 기술이다. 그림 1은 컴퓨터 포렌식스의 영역을 나타낸다[2].



<그림 1> 컴퓨터 포렌식스 영역

ESM(Enterprise Security Management)과의 차이점에 대해 의문점을 갖는 사람들도 있으나, ESM의 경우 보안제품간의 상호호환성을 바탕으로 관리할 수 있는 제한된 영역을 통제하는 시스템인 반면, 컴퓨터 포렌식스의 경우 침해사고대응 방법을 위해 여러 문제점들을 분야별로 구분시켜 놓음으로써 향후 침해사고 발생시 증거를 획득, 보존하여 법적 대응이 가능하도록 하는 시스템이라 할 수 있다.

3.1 컴퓨터 포렌식스 방법론

일반적으로 컴퓨터 범죄 관련 증거자료를 대상으로 한 컴퓨터 포렌식스 분석 방법론은 크게 역추적을 통한 방법과 증거물 복원을 통한 컴퓨터 포렌식스로 구분할 수 있다. 역추적을 통한 컴퓨터 포렌식스 방법에서는 이벤트가 발생한 근원지 또는 위치를 찾아가는 방법에 관한 사항을 제공한다. 컴퓨터범죄와 관련된 증거를 수집하고 이를 분석하여 근원지에 해당하는 IP 주소 등을 역추적한다. 그리고 근원지가 파악되면 이를 문서화하여 최종적인 증거물로 채택한다. 본 방법론에서 수행되는 과정을 단계별로 제시하면 다음과 같다[2,11].

- 1단계: 관련된 증거 자료 수집
- 2단계: 키워드 분석
- 3단계: 출처, 위치, 저장장소 및 근원지 파악
- 4단계: 증거물에 대한 문서화

증거물 복원을 중심으로 한 컴퓨터 포렌식스 방법은 관련 증거자료를 수집하여 데이터 복구 과정을 수행하고, 필요로 할 경우 암호화된 데이터에 대한 복호과정을 수행하여 증거물에 해당하는 데이터의 특성에 따라 수사하는 방식이다

- 1단계: 관련된 증거 자료 수집
- 2단계: 데이터 복구 및 암호 제거
- 3단계: 포맷 분류 및 은닉 자료 검색
- 4단계: 증거물 정리 및 문서화

3.2 포렌식스 시스템 분석방법

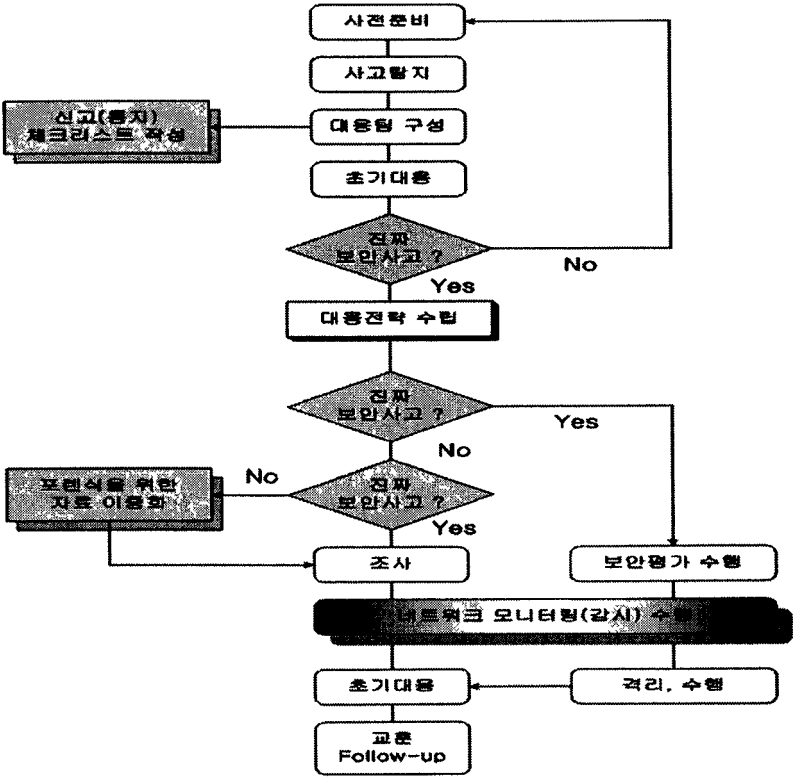
컴퓨터 포렌식스를 이용한 시스템 분석 방법에는 증거 보존 및 분석을 위한 시스템 분석 방법과 해킹과 같은 공격 흔적을 찾기 위한 무결성 도구를 이용한 방법, 그리고 공격기법을 분석하여 침해 여부를 판단하고 로그 파일 분석 및 복구를 통한 증거 수집을 이용한 방법 등이 있다[12,13].

- 분석 시스템을 이용한 분석방법
- 공격 흔적을 보존하기 위해 수행중인 프로세스 상태 및 포트, 현재 네트워크정보, 사용자와 터미널에 대한 로그 정보, 현재 사용자, 현재까지 변경된 모든 파일 등을 조사해야 한다
- 무결성 도구를 이용한 시스템 변조 유무 확인 방법
- 공격기법 및 웜바이러스(바이러스 포함)등을 분석하는 방법
- 공격자가 삭제한 파일이나 데이터를 복구하여 증거를 수집하는 방법
- 로그파일을 점검함으로써 파일의 유출 및 도난 여부를 확인하는 방법
- 디스크 복구를 통한 증거 수집 방법

3.3 침해사고 대응절차

침해사고대응을 할 때 일반적인 접근 방법은 "Incident Response"의 저자 Kevin Mandia과 Chris Prosise는 침해사고 대응의 일반적인 절차와 기능을 사전 준비단계, 사고 탐지단계, 초기 대응단계, 대응전략 수립단계, 포렌식스를 위한 자료 이중화 단계, 조사 단계, 보안평가 수행단계, 네트워크 모니터링 단계, 복구, 보고,

사후조치 단계 등 11단계로 그림 2와 같이 구분한다[2].



<그림 2> 침해사고 대응절차도

■ **사전준비 단계**

향후 과정을 원활히 수행하기 위한 과정으로써 필요한 프로그램과 장비를 준비하거나 사고 대응팀을 구성하고 이들의 역할을 정하며, 내부 규칙을 마련한다.

■ **사고 탐지 단계**

사고의 인지, 탐지는 사건해결의 첫 시발점이다. 이것들은 주로

IDS, F/W 또는 사용자의 인지에 의해서 알게 되는 것이 보통이며, Tripwire 와 같은 시스템 파일 체크섬을 확인해 주는 프로그램에 의해서도 가능하다.

■ **초기 대응단계**

초기 대응단계에서 사고 대응팀이 소집되어야 하며, 모든 작업은 책임자의 책임 하에 철저히 통제되어야 한다. 이 단계에서는 컴퓨터의 재부팅 시에 사라질 수 있는 휘발성 데이터를 수집하는 것 등이 포함된다.

■ **대응전략 수립 단계**

이 단계는 초기 대응단계에서 파악된 상황을 토대로 구체적으로 어떤 조치를 취할 것인지를 결정하는 단계이다. 사고를 내부에서 처리할 것인지 아니면 수사기관에 신고할 것인지도 이 단계에서 결정해야 할 사항이다.

■ **포렌식스를 위한 자료 이중화 단계**

컴퓨터 포렌식스는 법적인 문제를 해결하기 위한 컴퓨터 법죄 수사 과학이다. 전통적으로 컴퓨터 포렌식스는 하드 디스크의 원본을 완전히 복제하여 분석하는 것으로, 컴퓨터의 부검이라고도 한다.

■ **조사 단계**

조사는 복제된 하드디스크나 운영중인 시스템의 로그파일에 대한 검사를 포함하여 최초 사고 발견자, 보안담당자에 대한 면접 조사 등 세부적인 사고조사 과정을 말한다. 일반적으로 이 단계는 다른 단계에 비해 가장 긴 시간이 소요되는 것이 보통이다.

■ **보안평가 수행 단계**

보안 평가는 앞의 과정에서 조사된 결과물을 토대로 보안상의 문제점을 평가하는 과정으로, 향후 사고방지를 위한 작업을 뜻한다. 사고의 형태와 원인에 따라 시스템이나 네트워크 차원에서

어떠한 문제가 있었는지 또는 관리상의 실수가 있지는 않았는지, 또는 전반적인 보안정책에 문제는 없는지 등의 항목들이 검토되며, 그 수행결과에 따라 정확한 조치를 취하게 된다.

■ **네트워크 모니터링 단계**

보안평가와 조치 후에 해당 조치의 적절성을 판단하기 위하여 상당기간 네트워크에 대해서 한층 강화된 모니터링이 수행되어야 한다. 안전성이 검증될 때 까지 평상시보다 강화된 보안수준을 적용하여야 한다.

■ **복구**

복구는 사고를 당한 시스템과 네트워크를 정상적인 상태로 환원시키는 작업이다. 해커가 설치한 프로그램과 파일을 제거하고, 백업 파일로 지워지고 흐트러진 자료를 원상회복시키는 등의 작업이 복구과정에 포함된다.

■ **보고**

사고대응 절차를 종료하는 시점에서 개별사건에 대한 별도의 보고서를 작성하고, 조치결과는 책임자에게 보고되어야 한다. 때때로 이 단계에서 수사기관에 대한 신고가 이루어지거나 법적인 대응이 본격적으로 이루어지기도 한다.

■ **사후조치 단계**

실질적으로 사고대응을 하면서 알게 된 필요한 조치를 실무에 반영하는 것이다.

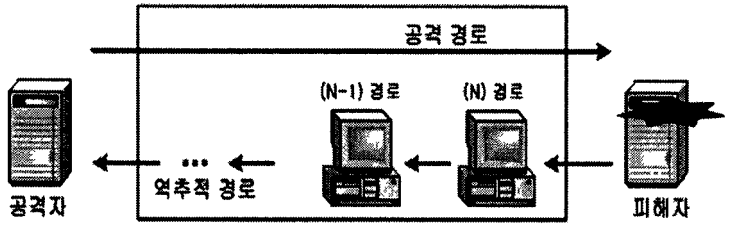
위에서 설명된 방법론은 각각의 중요한 의미를 지니고 있으나, 작업순서가 반드시 설명된 순서대로 진행되어야 하는 것은 아니다. 좀더 이해하기 쉬운 대응절차가 많이 있으며 그 중에 워싱턴 대학의 Dave Dittrich가 제시한 사고대응 6단계 모형은 매우 간결하고 많이 이용되고 있으며 비즈니스 관점에서의 접근방식을 취하였다.

Dittrich는 그 단계를 사전준비 인지, 차단, 근절, 복구, 후속조치 등 6가지로 구분하였다.

4. 역추적 기술

공격자는 자신의 위치가 노출되는 것을 피하기 위해 보안이 취약한 여러 호스트들을 공격한 후 최종 목적지를 우회적으로 공격하는 것이 일반적이다. 이러한 경우 네트워크상의 실제 공격자의 위치를 탐색하는 기술을 역추적이라 하며, 침입자의 확인과 증거 확보를 위한 분석 작업을 자동으로 수행하여 공격자의 실제 위치를 탐지하기 위한 시스템을 침입자 역추적 시스템이라 한다[9].

그림 3은 역추적 개념도를 보여주고 있다. 공격자가 자신의 시스템에서 N 개의 경유 시스템들을 해킹하고, 피해자의 시스템을 마지막으로 공격하였다고 가정하면 공격자의 시스템까지 역추적하기 위해서는 N 개의 시스템을 역으로 추적하는 것이 가능해야 한다.



<그림 3> 역추적 개념도

역추적 기술은 일반적으로 IP 주소가 변경된 패킷의 실제 송신 위치를 추적하는 IP 패킷 역추적 기술과 공격자가 자신의 위치를 숨기기 위해 우회공격을 시도하는 경우 공격자의 근원지를 추적하는 TCP 연결 역추적 기술로 분류되며 표 2와 같다.

<표 2> 역추적 기술의 분류

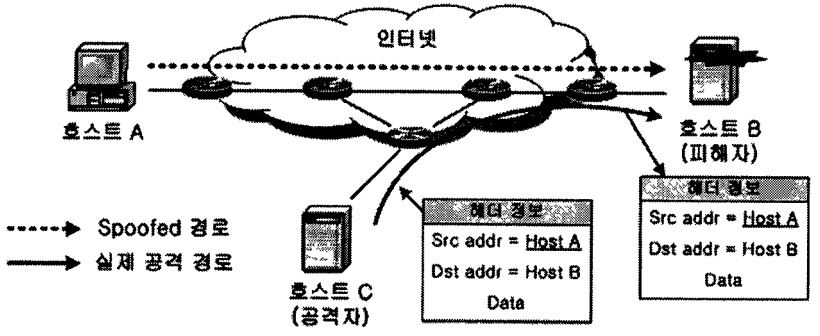
	IP 패킷 역추적 기술	TCP 연결 역추적 기술	
		호스트 기반	네트워크 기반
방법	공격자가 전송하는 패킷에 해당 패킷을 전달한 라우터를 표시하여 공격자를 추적	■ 각 호스트로부터 수집한 정보를 기반으로 하여 공격자를 추적	■ 네트워크 상의 송수신 되는 패킷에서 역추적을 수행할 수 있는 정보를 추출하여 공격자를 추적
특징	DoS나 DDoS 공격에서 IP 주소를 변경한 공격자의 실제 위치를 찾는데 주로 사용	■ 역추적을 위한 모듈을 네트워크 상의 모든 호스트에 설치하는 기법 ■ 우회공격의 근원지를 찾는데 사용	■ 역추적을 위한 모듈을 네트워크 상에서 송수신 되는 패킷을 확인할 수 있는 곳에 설치 ■ 우회공격의 근원지를 찾는데 사용

<표 2> 역추적 기술의 분류

단점	패킷의 끝에 노드의 주소를 계속 첨부해야 하기 때문에 라우터에 과부하를 초래	■ 네트워크 상의 모든 호스트에 역추적 모듈의 설치가 필요 ■ 역추적 경로 상에서 하나의 시스템이라도 역추적 정보를 얻을 수 없다면 역추적이 불가능	■ 네트워크 상의 패킷들로부터 생성되는 정보의 순서관계 및 동기화가 매우 어려움 ■ 네트워크 상에서 발생 하는 모든 연결에 대한 정보를 지속적으로 보유 하고 있어야 하는 문제 발생

4.1 IP 패킷 역추적 기술

IP 주소를 변경하면 TCP 연결을 유지할 수 없는 취약점이 발생하여 일방적인 패킷 송신만으로도 공격이 가능하기 때문에 IP 주소가 변경된 패킷은 서비스 거부(DoS: Denial of Service) 공격이나 분산 서비스 거부(DDoS: Distributed Denial of Service) 공격에 주로 사용된다.

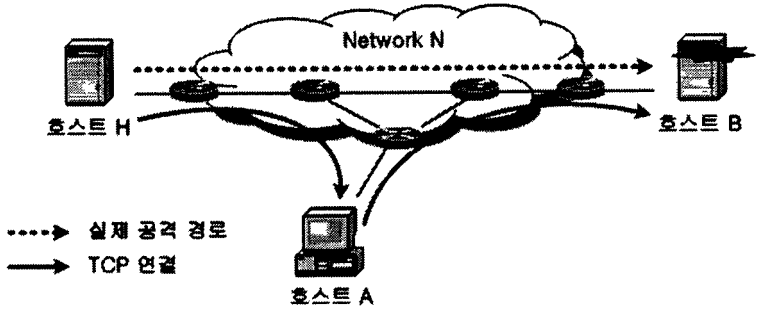


<그림 4> 패킷 마킹기법을 이용한 역추적

이러한 서비스 거부 공격에 대응하기 위한 IP 패킷 역추적 기법은 그림 4에서 볼 수 있듯이 공격자가 전송하는 패킷에 해당 패킷을 전달한 라우터를 모두 표시하여 공격자를 추적할 수 있게 하는 패킷 마킹 기법을 이용한 연구가 대표적이다 이 기법은 네트워크에서 패킷이 전송되는 동안 경유한 모든 라우터의 IP 주소를 패킷에 마킹한다. 침해사고 발생 시 마킹된 패킷을 받은 피해 호스트에서는 마킹된 라우터 주소 정보를 바탕으로 패킷이 지나온 경로를 재구성하고 네트워크 상에서 공격자의 근원지를 찾아가는 기법이다.

4.2 TCP 연결 역추적 기술

공격자는 침입시도의 성공 여부와 상관없이 최대한 자신에 대한 정보가 알려지지 않도록 다양한 방법을 사용한다. 특히, 목적 호스트를 공격하는데 공격자 자신의 시스템에서 직접 공격하는 것이 아니라, 여러 다른 시스템들을 경유하여 공격자의 위치를 감추는 방법을 사용한다. 이와 같이 어떤 공격자가 특정 시스템을 공격할 때 다른 시스템들을 경유하여 공격하는 것을 우회공격이라 한다[13].



<그림 5> 우회공격

즉, 우회공격은 그림 5와 같이 공격자가 최종 침입 대상 호스트를 공격하는데 직접 호스트 B로 침입을 시도하지 않고, 다수의 중간 시스템을 경유하여 침입을 수행하는 공격을 의미한다. 이러한 우회공격에서 경유된 시스템들로부터 침입 정보를 획득하여 실제 공격자의 위치를 역추적 하는 시스템을 우회공격 근원지 역추적 또는 연결 체인 역추적 기술이라 한다.

TCP 연결 역추적 기술은 표 3과 같이 호스트 기반 연결 역추적 기술과 네트워크 기반 연결 역추적 기술로 분류되고, 다시 수동적인 방법과 능동적인 방법으로 분류된다[9,10].

<표 3> TCP 연결 역추적 기술 분류

	수동적인 방법	능동적인 방법
호스트 기반	DIDS CIS AIAA	Caller ID
네트워크 기반	Thumbprint-based Timing-based Sequence Number-based	IDIP, CITRA, AN-IDR SWT **MTBS(제안방식)**

호스트 기반은 네트워크 상의 각 피해 시스템으로부터 수집한 정보를 기반으로 경유한 모든 시스템을 분석하여 공격자를 추적하는 방법이고, 네트워크 기반은 네트워크 연결 특성으로 연결체인에서 애플리케이션 레벨의 내용은 변하지 않는다는 점을 이용하여 공격자를 추적하는 방법이다.

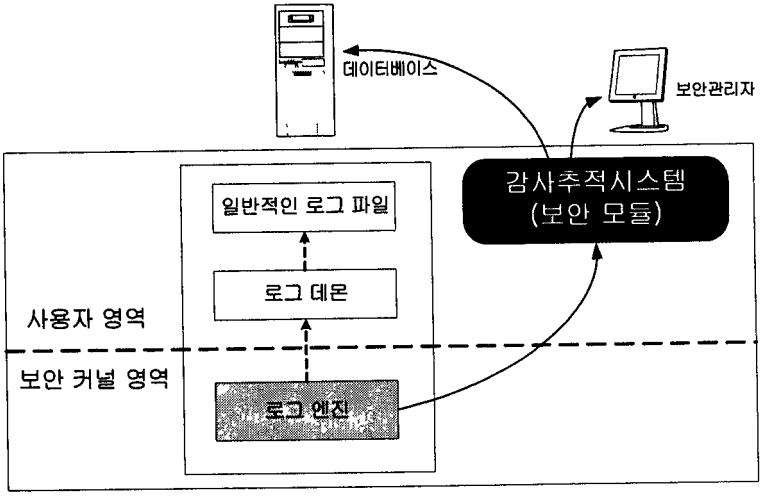
수동적인 방법은 피해 시스템에서 수동적인 모니터와 네트워크 트래픽을 비교하여 공격자를 추적하는 방법, 확실한 증거 자료 없이 역추적을 수행하고, 능동적인 방법에서는 사용자가 요구하는 기능을 수행할 수 있는 프로그램 코드를 패킷(Active Packet)으로 구성하여 전송하는 방법, 확실한 증거 자료를 바탕으로 역추적을 수행한다.

5. 증거포착 메커니즘 설계

본 논문에서는 정보전 대응을 위한 증거포착 메커니즘 설계를 위하여 커널 레벨에서의 로그 엔진 기술을 적용하였으며, 해당 보안정책을 적용한 후 안전한 데이터베이스로 저장되어 컴퓨터 포렌식

스 자료와 추적 시스템의 기본적인 자료로 사용하도록 설계하였다. 그림 6은 보안 커널기반의 감사/추적 시스템 구성을 보여준다. 이 시스템은 리눅스 운영체제에 다음과 같은 기능의 구현을 고려하였다.

- 운영체제 수준에서의 강제적 접근 통제(Mandatory Access Control)
- root 권한의 제한
- 커널 모드의 안전한 추적/감사 기능 제공
- 시스템 관리자와 보안 관리자의 역할 분리
- 네트워크에 의한 접근 통제



<그림 6> 감사/추적 시스템 구성도

5.1 로그 엔진

커널 모듈에서 보내는 로그 정보를 DB파일에 저장하기 위해서

커널 영역과 유저영역사이에 통신 인터페이스로 Character Device를 사용 한다.

<표 4> 로그 파일 DB 저장 알고리즘

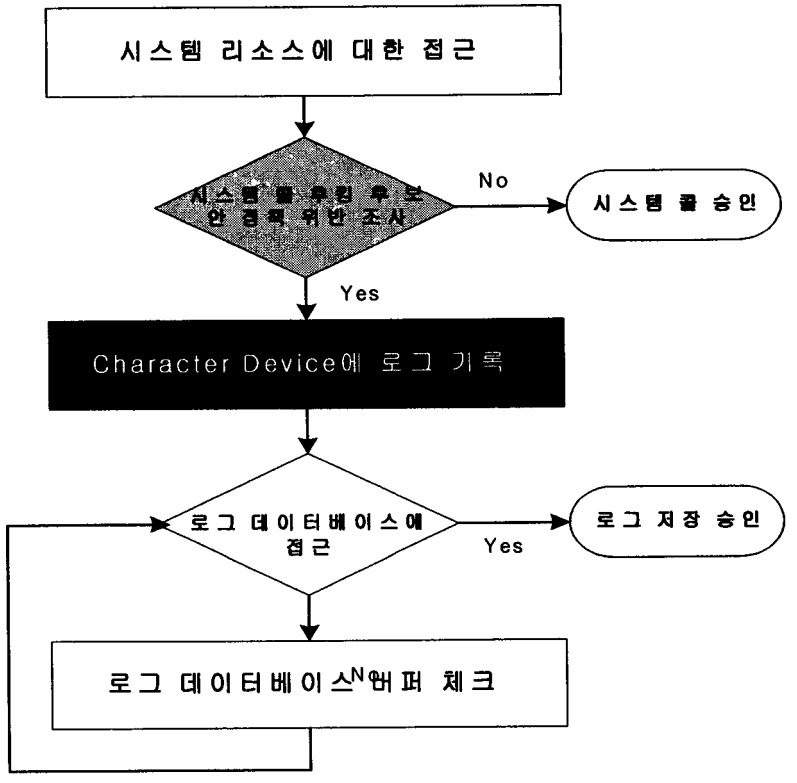
```
memset(object_path, '\0', PATH_MAX),
 if( SecuOS_Check_Base(dentry,SECUOS_WRITE) > 0 ) {
  sprintf(error_msg,"rmdir error no permission
SECUOS_WRITE");
  secuos_log(2,__FUNCTION__ , SecuOS_Absolute_Path(dentry, object_path), error_msg),

  if(!error_flag)
     path_release(&nd),
   putname(name),
   return -1,
}
```

커널 모듈에서 나오는 로그 정보를 로그 데몬이 Character Device를 3초 단위로 로그 메시지가 있는지 확인한다. 메시지가 있다면 실시간으로 DB파일에 저장한다. 이러한 커널 레벨의 로그 저장 방식은 실시간으로 저장하여 능동적인 대응에 필요한 추적 및 감사 자료로 활용되며, 컴퓨터 포렌식스를 위한 기초 자료로 사용된다. 표 4는 해당 알고리즘을 나타내며 <그림 7>은 Character device에 로그가 저장되는 과정을 도식화한 다이어그램이다.

5.2 보안 감사 모듈

보안 모듈은 커널 소스 수정이 필요 없는 커널 모듈 형식으로 커널에 애드-온 되도록 설계하였다. 보안 모듈은 참조 모니터링을 통한 강제적 접근 통제 구현과 Capability를 통한 네트워크 서비스 프로그램 제어를 제공하여 접근 통제 기능이 강화되었다.



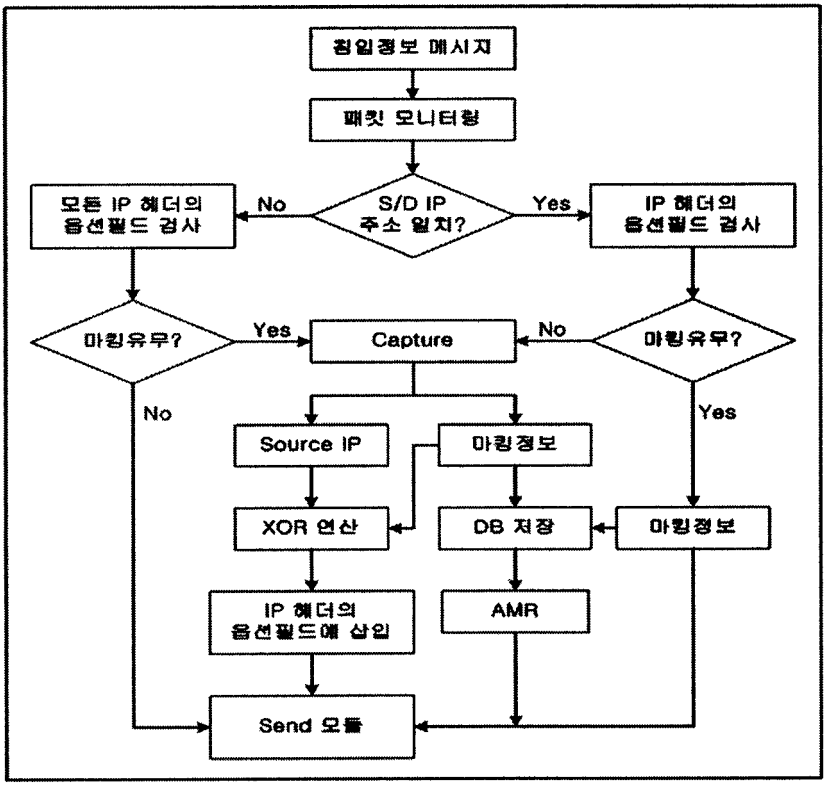
<그림 7> Character Device 로그 저장

참조 모니터링은 임의의 프로세스가 시스템 자원에 접근할 경우 실제시스템 콜을 후킹(hooking)한 시스템 콜이 호출되고, 후킹 된 시스템 콜에서는 접근 시도한 주체가 객체에 대해 요청한 권한이 있는지 체크하게 된다. 시스템 콜뿐만 아니라 커널에서 심볼 테이블에 등록한 파일 오퍼레이션 심볼에 대해서도 후킹을 시도 한다.

시스템 콜을 후킹 후, 그 시스템 콜을 호출한 주체(Subject)가 보안 정책에서 해당 권한이 명시되어 있으면 원래의 시스템 콜을 호출할 수 있도록 해주며, 보안 정책에 명시되어 있지 않으면 그 주

체에 해당하는 정보(level, time, uid, gid 등)를 Charater Device에 쓰게 되며, 상주해 있는 로그 데몬이 Character Device에 쓰여진 로그 정보를 DB 파일에 저장하게 된다. 보안 정책은 주체나 객체에 대한 접근 권한과 root 권한을 가진 사용자로 하여금 시스템이나 접근 기록을 변조 또는 삭제되지 않도록 설정하였다.

5.3 보안 추적 모듈



<그림 8> MTBS의 흐름도

제안된 MTBS(Marking TraceBack System) 모듈은 로그 데이터베이스에 저장된 자료를 기반으로, 해당 IP를 추적하여 침입자의 경로를 알아내는 모듈이다. MTBS는 크게 응답패킷 Capture 모듈, 마킹 Write 모듈, 마킹 패킷 Send 모듈로 구성된다. 또한, 각 경유하는 호스트의 IP 주소를 저장하기 위한 DB와 분산된 MTBS에서 경유 호스트와 공격자의 정보를 알리기 위한 AMR(Alert Message Report)이 존재한다. 그림 8은 MTBS의 흐름도를 나타낸다.

6. 증거포착 메커니즘 실험

6.1 감사를 위한 로그 정보 수집

서버 측의 에러 로그의 정보를 기반으로 침입자를 역추적 할 수 있는 자료로 활용하며, 침해사고 대응을 위한 컴퓨터 포렌식스의 중요한 자료가 된다. 이 로그 파일은 커널기반의 안전한 파일로 저장되게 되며, 무결성 보장을 위하여 별도의 데이터베이스에도 추가적으로 저장된다.

6.2 보안 정책 설정

보안 정책 정보는 TCSEC에서 정의한 C2 레벨 이상의 보안성을 만족시키기 위한 감사 자료 생성 기능을 제공하며, 모든 감사 이벤트에 동일한 포맷의 감사 자료를 생성한다. 또한 보안 모듈이 올라가 있는 리눅스 서버에 설정된 보안 관련 정책을 보여준다. 리스트 창에 나타난 보안 정책은 일반 정책과 프로세스 보호 관련 정책, 그리고 Bind 서버에 관련한 정책으로 구분지어 나타내어진다

<표 5> 보안 정책 설정

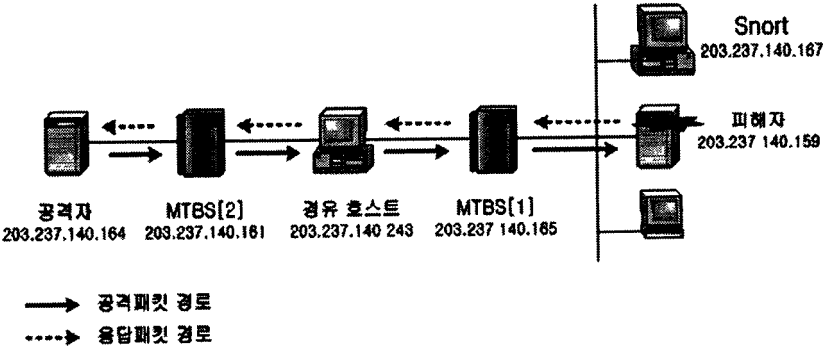
```
555064 769 /bin/login 1 0 229841 769 /etc/shadow 0-0
555064 769 /bin/login 7 0 767060 769 /var/log/lastlog 0-0
391825 769 /usr/sbin/sshd 1 0 229841 769 /etc/shadow 0-0
391825 769 /usr/sbin/sshd 16 0 -1 10 CAP_NET_BIND_SERVICE 0-0
.. ..
343198 769 /usr/bin/procmail 16 0 -1 10 CAP_NET_BIND_SERVICE 0-0
327938 769 /root/project/log_daemon/secuos_logd 16 0 -1 31 CAP_PROTECTED 0-0
```

기존 보안 정책을 나타내 주는 것뿐만 아니라, 보안 관리자가 보다 쉽게 정책을 추가하거나 삭제, 수정을 가능하게 해준다. 표 5는 보안 정책의 설정 내용이다.

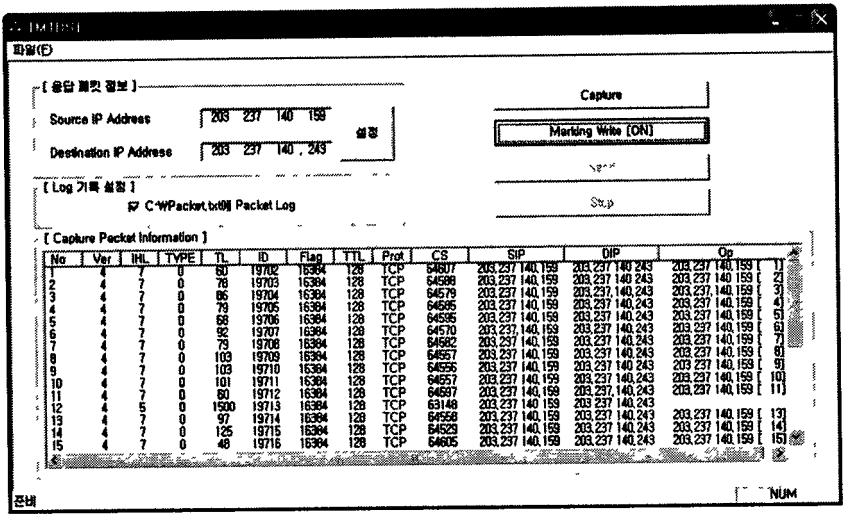
6.3 역추적을 통한 증거 수집

감사 모듈에 의해 저장된 로그 정보를 기반으로 공격에 대한 응답패킷을 Capture하기 위해 침입정보에서 Source IP와 Destination IP의 주소를 교환하여 MTBS[1]의 응답패킷의 정보에 입력한다. 이것은 우회공격의 연결특성에 따라 공격에 대한 응답패킷은 공격경로의 역방향으로 전달되기 때문이다. 실험환경은 그림 9와 같다.

<그림 10>은 MTBS[1]에서 Capture한 응답패킷에 Source IP 주소와 옵션필드를 XOR 연산하여 그 결과 값을 IP 헤더의 옵션필드에 새롭게 마킹한 결과이다. 마킹한 패킷은 Send 버튼을 통해 목적지 주소로 보낸다.



<그림 9> 실험 환경



<그림 10> 패킷을 마킹한 결과

MTBS[2]에서는 Source IP 주소와 옵션필드의 마킹여부를 검사하여 마킹이 존재하는 경우 이를 Capture한다. Capture된 옵션필드에 다시 경유 호스트의 주소를 마킹하기 위해 MTBS[2]는 응답패킷에서 Source IP 주소와 옵션필드를 XOR 연산하여 그 결과 값을

IP 헤더의 옵션필드에 새롭게 마킹한다. 그리고 Capture Packet Information에서 Destination IP 주소를 파악할 수 있으므로 마킹한 결과를 목적지 주소로 보낸다. 그리고 MTBS[2]는 Source IP 주소가 전송되는 패킷들을 모니터링 하여 옵션필드가 존재하는지 검사한다. 만약 존재하는 경우 전송했던 패킷의 옵션필드와 일치하는지 검사한다.

7. 결론

현대의 전쟁은 범국가적으로 산업전반에 걸쳐서 이루어지고 있으며, 이중 첨단 정보기술 기반의 사이버 공간을 통한 공격은 사이버 테러라는 새로운 형태의 침해사고를 만들어 냈다. 이러한 침해사고는 민간부문을 넘어서 군사부문까지 확대되어 과거의 전쟁개념과는 달리 물리적인 파괴가 아닌 국가의 신경조직인 정보통신망, 주요기반구조의 컴퓨터들을 파괴 또는 무력화 시켜 목적을 달성하는 새로운 형태로 확산되었다

본 논문에서는 정보보안 침해사고로부터 전자적인 현상에 의하여 과학적으로 그 원인을 진단하고 분석하여 법의학적인 증거를 제시하고 대응할 수 있는 컴퓨터 포렌식스 기술을 기반으로 증거를 수집하고 분석하여 침해사고 발생시 추적하여 원천적인 대응이 가능한 증거포착 메커니즘을 설계하였다. 설계된 증거포착 메커니즘은 리눅스 운영체제에 대해 기존 커널의 변경 없이 LKM (Loadable Kernel Module)기법을 통해 동적으로 로딩이 가능하도록 설계되어, 커널의 재수정이나 시스템의 리부팅이 없이 적용할 수 있으며, 침입 탐지 시스템과 같은 외부의 프로세스가 생성한 감사 자료를 활

용할 수 있는 인터페이스를 가지고 있다. 이러한 감사 자료를 바탕으로 마킹 기반의 역추적 시스템 구현이 가능하고, 추후 발생할 수 있는 보안침해 사고에 대비한 컴퓨터 포렌식스 자료로의 사용은 상당히 효율적이라 할 수 있다. 현재의 모든 운영체제나 네트워크는 소극적 방어이기 때문에 제안 시스템에서는 컴퓨터 포렌식스나 실시간 역추적을 제공함으로써 능동형 방어 기술의 근본적인 기법을 제공할 수 있다.

참고문헌

박태규 · 임연호. 2001. "리눅스 커널 기반의 안전한 OS 개발".

최용락 · 고병수 · 박명찬. 2003. "정보대응을 위한 컴퓨터 포렌식스 기반 모의실험". 『군사학연구』. 제1호. pp.391-421. 대전대학교 군사연구원.

박상서 · 박춘식. 2002. "정보전 위협과 사례". 정보보호학회지. 12권 6호. 한국정보보호학회.

박상서 · 김현수. 2003. "미국의 국가 사이버보안 및 국방 정보전 대응체계". 한국사이버테러 정보전학회지. pp.68-77. 한국사이버테러정보전학회.

최양서 · 서동일 · 손승원. 2003. "역추적 기술 동향: TCP Connection Traceback 중심". ITFIND 주간기술동향. 1079호.

Kretzer, 2002, *"Air Force Information Warfare Center: Taking IW Combat Power to the Warfighter"*, InfowarCon.

Martin Libicki, 1995, *"What is Information Warfare?"*.

White House, Feb. 2003, *"The National Strategy to Secure Cyberspace"*.

White House, Feb. 2003, *"The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets"*.

Kevin Mandia & Chris Prosise, *"Incident Response - Investigating Computer Crime"*, McGraw-Hill.

Eoghan Casey, 2001, *"Handbook of Computer Crime Investigation: Forensic Tools & Technology"*, Academic Press.

Eoghan Casey, 2001, *"Digital Evidence and Computer Crime"*, Academic Press.

John R. Vacca, Michael Erbschloe, 2002, *"Computer Forensics: Computer Crime Scene Investigation (With CD-ROM)"*, Charles River Hedia.

Executive Order 13228 of Oct. 8, 2001, *"Establishing the Office of Homeland Security and the Homeland Security Council"*.

A Design of Electronic Evidence-seizure Mechanism for the Response of Information-warfare

Park, Myung-Chan · Lee, Jong-Seob · Choi, Yong-Rak

The forms of current war are diversified over the pan-national industry. Among these, one kind of threats which has permeated the cyber space based on the advanced information technology causes a new type of war. C4ISR, the military IT revolution, as a integrated technology innovation of Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance suggests that the aspect of the future war hereafter is changing much. In this paper, we design the virtual decoy system and intrusion trace marking mechanism which can capture various attempts and evidence of intrusion by hackers in cyber space, trace the penetration path and protect a system. By the suggested technique, we can identify and traceback the traces of intrusion in cyber space, or take a legal action with the seized evidence.

Key words: Computer Forensics, Traceback, Information-Warfare