「정보학연구」 제10권 제3호 2007년 9월(pp.93-120)
The Journal of Information Technology, Vol.10, No.3

스마트홈 환경에서 컴퓨터 포렌식스의 디지털 증거 무결성 보증 메커니즘

A Mechanism for Securing Digital Evidences of Computer Forensics in Smart Home Environment

이 종 섭 (Lee, Jong Sup)*·박 명 찬 (Park, Myung Chan)*·
장 은 겸 (Jang, Eun Gyeom)*·최 용 락 (Choi, Yong Rak)*·이 범 석(Lee, Bum Suk)**

목 차

Abstract

A Smart Home is a technically expanded from home network that gives us a comfortable life. But still there is a problem such as mal function of devices and intrusions by malicious parties since it is based on home network. The intrusion by malicious parties causes a critical problem to the individual's privacy. Therefore to take legal actions against to the intruders, the intrusion evidence collecting and managing technology are widely researched in the world. The evidence collecting technology uses the system which was damaged by intruders and that system is used as evidence materials in the court of justice. However the

* 대전대학교 컴퓨터공학과
** 혜천대학 컴퓨터멀티미디어콘텐츠과

collected evidences are easily modified and damaged in the gathering evidence process, the evidence analysis process and in the court. That's why we have to prove the evidence's integrity to be valuably used in the court.

In this paper, we propose a mechanism for securing the reliability and the integrity of digital evidence that can properly support the Computer Forensics. The proposed mechanism shares and manages the digital evidence through mutual authenticating the damaged system, evidence collecting system, evidence managing system and the court(TTP: Trusted Third Party) and provides a secure access control model to establish the secure evidence management policy which assures that the collected evidence has the corresponded legal effect.

Key words: 적응적 배경생성, 객체추적, Digital Evidences, Computer Forensics, Smart Home

Ⅰ. 서론

최근 정보통신 관련 기술의 비약적인 발전으로 비즈니스 커뮤니케이션의 70%가 전기, 전자적으로 이루어지고 있다. 이에 따른 순기능과 더불어 각종 해킹사고 및 사이버 범죄와 같은 역기능은 갈수록 증가하고 공격수법 또한 지능화, 다양화되고 있다. 이러한 보안 침해사고에 따른 사생활 침해로 인한 인권 문제와 경제의 위협요소로 작용하여 기업의 생존까지 영향을 미치고 있다[1].

시스템 침해의 문제는 가정 내의 다양한 디지털 기기와 PC 관련 제품들을 하나의 네트워크로 연결하여 상호 정보 교환과 공유를 가능케 하는 홈네트워크 환경에 영향을 미친다. 또한 홈네트워크에 지능과 상황인식 개념을 추가하여 발전된 형태인 스마트홈 환경에 치명적인 영향을 미친다. 스마트홈과 홈네트워크는 개인의 예민한 정보까지 포함을 한다. 그러므로 시스템 오작동 및 침해의 범죄행위에 대해서 치명적인 피해가 발생한다.

이에 따라 미국을 중심으로 기술 선진국들은 보안 침해사고에 대하여 디지털 전자적 증거를 수집, 분석 및 대응할 수 있는 컴퓨터 포렌식스 기술 개발에 집중하고 있다. 그리고 다양한 보안 침해사건의 사실관계를 확정 또는 증명하기 위한 법의학적 해석과 안전한 비즈니스 커뮤니케이션의 제도적인 정착을 위하여 국가적 전략산업으로 개발하고 있다. 이러한 활동들을 뒷받침할 수 있는 핵심적 컴퓨터 포렌식스 도구의 개발분야는 새로운 전문적 기술의 인기 직종으로 부상하고 있다.

정보보호 사고는 법적 판단에 필요한 증거자료가 결정적인 역할을 하고 있는 상황에서 사이버 범죄 대처와 기업의 정보자산 보호에 큰 역할을 할 수 있도록 내부자 정보유출을 비롯한 정보보안 사고 발생시의 상황을 그대로 재현할 수 있는 보안사고 원인 분석 기능을 갖추어, 모든 트래픽과 다른 시스템간의 연관성을 저장한 후 감식 기술로 분석하여 당시 상황을 그대로 재현할 수 있는 시나리오를 도출할 수 있는 기법을 필요로 한다.

현재 컴퓨터 포렌식스 도구는 EnCase와 TCT가 대표적이다. 대다수의 포렌식스 도구들은 삭제된 파일을 복구할 수 있는 복구기능, 다양한 방식으로 문자열이나 파일을 검색할 수 있는 검색기능, NIST(National Institute of Standard and Technology)와NDIC(National Drug Intelligence Center)에서 배포한 NSRL(National Software Reference Library)과 HashKeeper Library를 이용한 파일추출기능, 파일의 Magic Number를 이용하여 속성이 변경된 파일을 검색하는 시그니쳐 분석기능, 효과적으로 보고서를 작성할 수 있도록 하는 레포팅 기능을 제공한다[2].

기존 포렌식스 도구들은 사이버 범죄 수사가 착수된 시점을 기준으로 범죄에 이용된 시스템을 압수

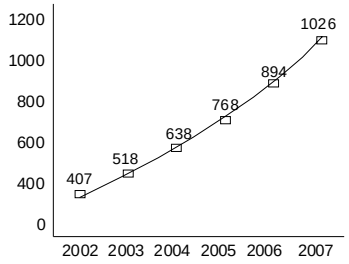
수색하여 법적 대응 증거를 도출한다. 그러나 법정 증거자료로 활용된 자료가 수사 대상시스템에서 수집된 증거인지에 대한 무결성 및 신뢰성에 문제점을 잠재적으로 가진다.

본 논문에서는 스타트홈 환경에서 발생할 수 있는 범죄 행위에 대해, 오작동 및 침해행위의 근거자료를 법정에서 시스템 침해의 증거로 효력을 발휘할 수 있도록 증거자료의 신뢰성 문제를 보증하기 위한 메커니즘을 제안한다.

Ⅱ. 관련 연구

1. 스마트 홈

스마트 홈은 이동통신, 초고속인터넷 등 유·무선 통신 네트워크를 기반으로 가정 내의 A/V, 데이터통신 및 정보가전기기들이 네트워크로 상호 연결되어 기기·시간·장소에 구애받지 않고 다양한 서비스를 제공받을 수 있는 가정환경을 구축하여, 편리하고, 안전하고, 즐겁고, 윤택한 삶을 제공할 수 있는 IT 기술 이용환경이라 할 수 있다. 그림 2.1은 스마트 홈 시장 전망(출처:Garrner Group 2002~2003 in-Star 2003)을 나타낸다.



<그림 2.1> 스마트 홈 시장 전망

가트너 그룹(Gartner Group)에 따르면 스마트 홈 세계 시장은 2002년 407억 달러에서 2007년에는 1,026억 달러 규모로 연평균 19%대의 성장이 예상된다.

최근 홈시큐리티의 중요성이 대두되면서 많은 업체들이 이와 관련된 제품과 서비스를 출시하고 있다. 특히 디지털 도어록과 인터넷 카메라, DVR 방재 센서 등을 이용한 보안 서비스들이 많이 소개되어 있다. 이러한 홈시큐리티에서 발생하는 보안 문제를 법으로부터 보호 받기 위한 정책 및 기술은 미비한 실정이다.

2. 컴퓨터 포렌식스 연구 동향

미국, 영국의 경우 절차를중시하는 체계와 사립탐정제도가 발달되어 있어 법률 집행 기관뿐 아니라 비영리기구, 일반 영리업체, 대학원등의 교육기관에서 전문적인 컴퓨터 포렌식스 교육과정을 신설해 전문가를 육성하고 있으며, 지침서 등의 문서도 잘 마련되어 있다.

컴퓨터 포렌식스를 위한 관련 연구기관은 대표적으로 미국 법무부, CFTT(Conputer Forensics Tool Testing), HTCN(High-Tech Crime Network), CERIAS, ASCLD, IACIS를 들 수 있다[3)4)5)].

- 미국 법무부: 전자증거물에 대한 압수 수색 절차 안내하는 가이드라인을 발행하였으며, 컴퓨터 범죄가 확산되자 기존의 CCIPS(Computer Crime and Property Section)를 개설하였다. 컴퓨터 범죄에 관련된 문서들을 비롯해 주요 인프라 보호 요령, 지적재산권 보호, 전자상거래의 법적 문제에 관한 세션들을 담고 있다.
- CFTT: NIST에서는 CFTT(Conputer Forensics Tool Testing) 프로젝트를 수행하고 있다. 이 프로젝트에서는 포렌식스 도구가 필수적으로 갖추어야할 기능에 대한 요구사항을 목록화 하고 그 기능을 잘 수행하는지에 대해 평가할 수 있도록 포렌식스 소프트웨어 도구를 평가할 수 있는 방법론을 제시하고 있다. 현재까지 디스크 이미징 도구가 갖추어야 할 몇 가지 요구사항을 정리하여 테스트 결과를 발표하였다.
- HTCN: 비영리 기구로서 컴퓨터 포렌식스에 관련된 교육 및 테스팅 기관 정보, 컨포런스, 세미나 등 교육정보, 컴퓨터 포렌식스 관련 도구 및 기술 자료들에 정보를 제공하고 있다.
- CERIAS: 컴퓨터 및 네트워크 보안, 통신 보안등에 대한 연구 및 교육활동에 있어 세계적으로 인정을 받고있는 퍼듀대학(Purdure University)의 센터이다. 기술적인 내용에 대한 연구뿐만 아니라, 교육, 법분야, 언어분야, 경제분야 문제들에 대한 관계와 그 의존성에대한 연구를 병행하고 있다.
- ASCLD: 컴퓨터 포렌식스를 수행할 수 있는 연구시설과 기관들을 심사하고자격을 승인해 주는 기관이다. 이를 위해 ASCLD는 연구시설이나 기관들이 컴퓨터 포렌식스를 수행함에 있어서 따라야 할 기준을 제정하여, 이러한 사항들을 이행할 것을요구하고 있다. 이 밖에도 Proficiency Testing 및 지속적인 교육과 트레이닝 활동을 규정해 놓고 있다.

- IACIS: 1989년 설립된 단체로 연방, 주, 지방, 국제 법률 집행기관의 컴퓨터 포렌식스 전문가들로 구성된 비영리 법인단체이다. IACIS에서는 컴퓨터 범죄 처리 절차를 만들어 컴퓨터를 압수하고 컴퓨터에서 전자적 증거물을 획득하는 방법을 확립했으며 교육과정을 설립해 포렌식스 전문가를위한 지속적인 훈련을 진행하고 있다.

3. 컴퓨터 포렌식스 도구 분석

1) EnCase

EnCase는 많은 양의 컴퓨터 증거를 쉽게 관리하고 파일 스택과 할당되지 않은 데이터를 볼 수 있는 GUI의 특징을 가지고 미 연방 법원의 EnCase를 통해 얻은 결과물을 법적인 증거로 채택한 판례로 인해 더욱 성능을 인정 받고 있는 도구이다[6].

EnCase의 주요 기능은 증거 자료의 다양한 파일 시스템 지원, 증거 자료의 무결성 보장, 유연한 이미지 추출 방법 제공, 사용자 정의 스트립트 작성을 통한 자동화 작업, 파일의 정확한 Timeline 추적, 삭제된 파일과 폴더 및 비 할당 클러스터 영역 검색 및 복구, 레포팅이다.

- 다양한 파일 시스템 지원
  윈도우(NTFS, FAT 16/32), 리눅스(ext2), 유닉스(UFS), MacOS 파일 시스템 분석가능
- 증거자료의 무결성 보장(Digital finger printing)
  증거 자료로서의 무결성을 보장하기 위해서 피해 시스템의 하드 디스크를 MD5 hash algorithm을 사용하여 digital finger printing(다양한 해쉬 알고리즘 지원)
- 유연한 이미지 추출 방법 제공
  다양한 이미지 추출 방법을 제공(Fast Blot을 이용한 bit 단위의 drive-to-drive 이미지 생성, Parallel Port를 이용한 이미지 전송, 활성화된 NIC을 통한 네트워크 전송지원)
- 사용자 정의 스크립트 작성을 통한 자동화 작업 가능
  EScript(스크립트 검색 도구)를 이용하여 숨겨진 E-Mail, NT Security event log, Internet History 등을 검색하고, 일반 텍스트와 HTML 형식을 지원하는 레포팅 기능과 삭제된 파일과 비할당 클러스터 영역 검색 및 복구 기능을 제공

2) TCT

TCT는 UNIX계열 시스템에서 수행되는 컴퓨터 포렌식스 소프트웨어로 1999년 Dan Farmer와 Wietse Venema에 의해 제작된 공개용 도구이다. TCT는 침해 사고 발생 당시의 이벤트 수집 및 분석을 보다 정확하고 수월하게 수행하기 위한 기능을 제공한다. 피해 시스템의 상태 정보에 대한 snapshot을 생성하며, 백업된 디스크 이미지 분석 및 파일 복구에 유용하게 사용할 수 있다[7].

TCT 구성 프로그램의 주요 기능은 <표 2.1>과 같다.

<표 2.1> TCT 구성 프로그램 기능

프로그램	설 명
grave-robber	피해 시스템의 휘발성 정보를 캡쳐한다. 네트워크 상태 정보, 주요 설정 파일, 일반 시스템정보 등을 수집
pcat	메모리에 로그된 프로세스를 수집
ils	파일시스템의 inode 정보를 수집, 기본적으로 지워진 파일에 대한 inode 정보를 제공, 다양한옵션을 사용하여 inode에 대한 정보를 수집
icat	지정된 inode number에 해당하는 파일의 내용을 출력
file	복구된 파일의 file type를출력
unrm, iazarus	파일시스템에서 할당되지 않은 디스크의 블록들을 분석하고 복구, unrm은 디스크에서 할당이 해제된 데이터 블록을 복구, lazarus은 unrm으로부터 raw 데이터를 분석하며 복구된 데이터 블록을 구조화 시키다.
mactime	파일의 접근, 수정 시간을 조사하고 파일시스템에 대한 timeline 생성

3) TCTUtils

TCTUtils는 TCT의 기능을 확장한 유틸리티로 Brian D. Carrier에 의해 작성되었다. 기존의 TCT가 file inode 정보만을 처리하는 반면에 TCTUtils를 사용하여 directory inode에 대한 정보를 수집할 수 있으며 디스크 이미지에서 파일 구조에 대한 정보를 수집할 수 있다. TCTUtils 구성 프로그램의 주요 기능은 <표 2.2>와 같다.

<표 2.2> TCTUtils 구성 프로그램 기능

프로그램	설 명
bcat	디스크 블록의 내용을 출력
blockcals	unrm으로 생성된 이미지의 블록넘버를 원래의 디스크 이미지에서의 블록넘버로 변환
fls	Directory inode 정보의 파일의 디렉토리 정보를 출력한다. 삭제된 디렉토리내의 하위 디렉토리와 파일들을 추출할 수 있다.
find_file	주어진 inode 값을 사용하는 파일 또는 디렉토리의 위치를 확인한다.
find_inode	주어진 이미지의 블록 number에 할당된 inode의 위치를 확인한다.
istat	지정된 이미지의 inode에 대한 상세 정보를 보여준다.

그 외의 도구로 Sleuth Kit와 Autopy forensics Browser은 TCT, TCTUtils 프로그램과 유사한 기능을 갖추고 있다. Sleuth Kit는NTFS, FAT, FFS, EXT2FS, EXT3FS를 지원해 다양한 파일 시스템을 분석할 수 있다. 또한 Autopy는 피해 시스템 분석을 진행하는데 있어서 작업을 용이하게 하기 위해 개발된 웹 브라우저 기반의 GUI 프로그램이다.

4. 보안 모델(BLP)

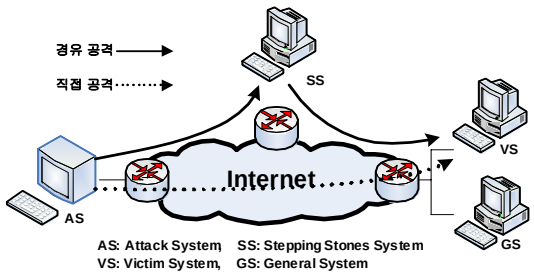
Bell과 Lapadula에 의하여 불법적인 정보유출을 보호하는 보안정책을 기반을 개발된 모델로서 정부기관이나 국방조직에서 가장 널리 사용되고 있는 최초의 수학적 모델이고, 강제적 정책하에서자료 보호를 위한 참조 모델이다. BLP 모델은 주체와 객체에 각각 보안등급을 부여하여 허가되지 않은 사용자로부터의 객체에 대한 접근을 금지한다. 보안 등급은 허용등급과 범주의 2가지 구성 요소로이루어진다. 허용등급은 TS(Top Secret), S(Secret), C(Confidential), U(Unclassified)의 4가지 요소로구성된 집합이며, 등급 순위는 TS > S > C > U 이다. 범주의 집합은 요소들의 비계층적집합의 부분 집합으로서 이 집합의 원소는 고려되는 환경에 의존적이고, 정보가 포함되거나 사용되는 응용분야와 관계가 있다.

주체는 어떤 정보를 갖고 있는 수동적 객체에 대하여 접근할 수 있는 시스템의 능동적 요소로서 사용자의 측면에서 동작하는 프로세스이다. 각 사용자는 접근허가(clearance)라는 보안 등급을 할당 받고, 이 등급이 지배하는 범위 이내에서 시스템에 로그인할수 있다. 그리고 그 사용자에 의하여 생성된 프로세스는 사용자가 로그인한 시점의 보안등급을 부여 받는다. 객체는 보호될 대상 정보로서 파일, 메모리 부분과 프로그램들을 생각할 수 있다. 범주의 집합은 BLP 모델의 범주집합과 비슷한 비 계층구조 집합의 부분집합이다.

Biba 모델은 BLP의 ss-property 및 *-property와 유사한 이원적 성질을 갖는다. 그러나 보안등급 사이에서 가지고 있는 관계는 반대이다. 즉, 두 가지 원칙 No Read-Down Integrity와 No Write-Up Integrity에 의하여 낮은 무결성의 객체로부터 더 높거나 또는 Incomparable 무결성 등급의 객체로 정보가 이동되는 것을 방지한다[7][8][9].

5. 기존 기술의 문제점

그림 2.2은 일반적인 네트워크환경에서 발생하는 공격 형태를 보여준다.



<그림 2.2> 일반적인 공격 형태

공격이 발생한 시점을 기준으로 피해 시스템, 가해 시스템, 경유 시스템으로 분류할 수 있으

며, 법과학 측면에서 컴퓨터 포렌식스 방법론은 수사착수, 증거식별, 증거 수집, 증거보존, 전송 및 저장, 수사종결의 절차를 따른다.

그림 2.2과 같은 환경에서 기존의 방법들이 갖고 있는 문제점들은 다음과 같이 3가지 측면으로 분석할 수 있다.

1) 시스템의 신뢰성에대한 문제

- VS 및 AS, SS 등 시스템 자체에 대한 신뢰성: 디지털증거를 생산하고 관리하는 시스템 자체에 대한 신뢰성으로 디지털 증거가 생성되기 이전에 이를 생성하는 시스템의 상태에 대한 신뢰성이 선행되어야 한다.
- 증거수집에 사용되는 컴퓨터 포렌식스 프로그램에 대한 신뢰성: 기존 포렌식스 도구는 각국의 디지털 범죄수사팀에서 EnCase, iLock, ACES를 많이 사용하고 있다. 하지만 표준화된 포렌식스 절차가 없어 모호성을 가진다.
- 디지털증거의 수집/보관에 대한 신뢰성: 디지털증거가 사고발생시에 수집한 증거자료와 법정에 제출한 증거 자료와 같다는 사실을 입증해야만 법적 효력을 받는다.

따라서 디지털증거를 생성하고 관리하는 시스템 자체에 대한 신뢰성, 디지털증거를 분석하고 수집하는 포렌식스 도구/시스템에 대한 무결성검증, 최종으로 법정에서 제출된 디지털증거가 원본과 같음을 증명할 수 있는 보안메커니즘이 필요하다.

2) 컴퓨터 포렌식스 적용상의 문제

- 기존의 컴퓨터 포렌식스 분야의 기술은 법집행기관의 법과학 실험실을 중심으로 수행: 전통적인 법과학적 컴퓨터 포렌식스는 대상시스템을 압수하여 증거를 분석한다. 법과학 실험실로 옮겨 온다는것은 시스템 운영상 매우 어려운 실정이다.

따라서 잘 설계되고 운영되는 전통적인 법과학 실험실이 증거의 신뢰성을 높이는데 크게 기여하는 것을 인정한다고 해도, 기술 변화가 극심하고 사건현장의 가변성이 높은 사이버범죄 현장에서 얻어지는 디지털증거에 대한 법과학 시험과 분석에는 그특성에 맞는 접근방법을 개발해야 한다.

3) 접근방식의 문제점

- 포렌식스 절차의 표준화 중심의 연구: 지금까지 발표된 컴퓨터 포렌식 분야의 연구 결과는 주로 절차의 표준화와 세부적인 증거수집 방법론이 제시되어 왔을 뿐이고 디지털 증거의 본질적인 속성에 초점을 맞춘 과학적인 접근방법에는 상대적으로 소홀히 하고 있다.

디지털증거의 신뢰성은 디지털증거의 원본 관리와 무결성 보증여부에 따라 결정된다. 디지털 증거의 원본관리와 무결성 보증 문제는 컴퓨터시스템이나 저장매체와는 독립적으로 디지털데이터의 본질적인 속성의 관점에서 컴퓨터 포렌식 분야의 연구에 있어서 포렌식 절차의 표준화와 증거수집 기술의 개발, 그리고 포렌식 도구 개발에 관한연구이다. 이와 함께 디지털증거의 신뢰성 보증을 위한 원본 관리와 무결성 보증에 관하여 보다 과학적인 접근이 이루어져야 할 것이다.

본 논문에서는 디지털 증거의 매체 독립적 속성과 법과학적 문제점을 컴퓨터 포렌식스 관련에서 분석하고 디지털 증거의 매체 독립적인 접근방법에 적합한 법과학적 디지털증거 무결성 보증 메커니즘을 제시하여 사이버범죄 수사절차와 침해 사고 대응과정에서 획득하는 디지털증거에 대한 신뢰성을 향상시키고자 한다.

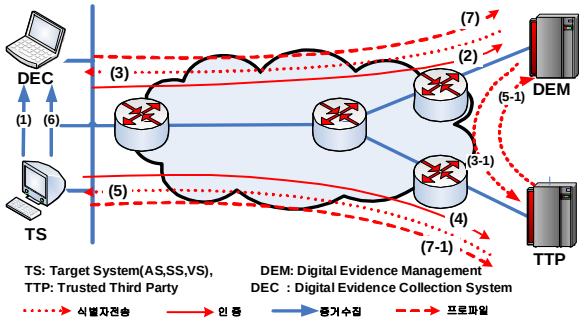
Ⅲ. 디지털증거 무결성 보증 메커니즘

1. 시스템 환경 및 구성

본 논문에서 제안하는 디지털증거 무결성 보증 메커니즘을 일반 네트워크 환경에 적용하기 위해서 디지털증거 관리 시스템(DEM), 디지털증거 수집 시스템(DEC) 및 신뢰할 수 있는 제3기관(TTP)으로 구성한다.

DEM은 네트워크상에서 발생하는 보안침해사고의 감시 및 접수 기능을 수행하고, 보안침해사고가 발생되면 대상시스템(TS)에 DEC를 설치한다. TS에 설치된 DEC는 TS에 내포된 디지털 데이터를 분석하여 디지털증거를 생성한다. 이때 생성되는 디지털증거는 DEM 및 TTP에 식별자를 요청하고, 수신된 식별자를 이용하여 디지털증거에 대한 프로파일을 생성한다. 생성된 프로파일 및 디지털증거는 TTP와 DEM에 전송하여 보관한다. TTP 및 DEM의 식별자는 DEC에 의해 생성되는 디지털증거의 무결성을 보증하는 역할을 수행한다.

제안 메커니즘은 디지털증거의 수사절차에 따라서 증거식별(1단계), 증거수집(2단계), 증거보존(3단계), 전송 및 저장(4단계)로 분류한다. 1/2/3단계는 DEC에서 수행하고, 4단계는 DEM에서 수행한다. 이때 3단계의 증거보존을 위한 식별자 생성 및 프로파일저장은 TTP에서 수행한다. 그림 3.1과 3.2는 증거물의 무결성 보증을 위한 처리 절차를 나타낸다.



<그림 3.1> 무결성 보증 시스템 구성도

TS	DEC	$(1) SI_{TS}$
DEC	DEM	$(2) EKU_{DEM}\left[EKR_{DEC}\left[KS_{CM}\right]\right] \| EKS_{CM}\left[CN_{DEC} \| N\right]$
DEM	DEC	$(3) EKS_{DEM}\left[CN_{DEM} \| EKR_{DEM}\left[H\left(CM_{DEM}\right)\right] \| CN_{DEC} \| N\right]$
DEM	DEC	$(3-1) EKU_{DEC}\left[EKR_{TTP}\left[KS_{MP}\right]\right] \| EKS_{MP}\left[CN_{DEC} \| CN_{DEM} \| N\right]$
DEC	TTP	$(4) EKU_{TTP}\left[EKR_{DEC}\left[KS_{CP}\right]\right] \| EKS_{CP}\left[CN_{DEC} \| N\right]$
TTP	DEC	$(5) EKS_{CP}\left[CN_{TTP} \| EKR_{TTP}\left[H(CN_{TTP})\right] \| TT \| CN_{DEC} \| N\right]$
TTP	DEM	$(5-1) EKS_{MP}\left[CN_{DEM} \| CN_{TTP} \| N\right]$
TS	DEC	$(6) Digital\_Data$
DEC	DEM	$(7) EKS_{CM}\left[DEI \| EKR_{DEM}\left[H(DEI)\right] \| CN_{DEM} \| N\right]$
DEC	TTP	$(7-1) EKS_{CP}\left[H(PI) \| CN_{TTP} \| N\right]$

<그림 3.2> 무결성 보증 절차

(1) DEC는 TS에 접속하여 시스템정보(SI)를 수집한다. 이때 수집되는 정보는 TS를 식별할 수 있는 H/W 및 S/W 고유값을 이용한다. 이후, DEC는 SI를 이용하여 CN_{DEC}(Case Number)을 생성하고, (2) DEM에 식별자를 요청한다. CN의 식별자 CN_{DEC}을 생성하여, (3) DEC 및 (3-1) TTP에 전송한다.

DEC는 수신된 CN_{DEC}을 보관하고, 이후, 프로파일 생성에 필요한 식별자를 사용한다. (4) DEC는TTP에 식별자 및 TT(Time-sTamp)를 요청한다. TT는 현재 수행되는 프로그램의 표준시간과 디지털증거 수집 시점으로 사용된다. TTP는 (3-1)에서 수신된 CN_{DEC}과 DEC에서 수신된 CN_{DEC}과 DEC에서 수신된 CN_{DEC}을 확인하고 같으면 TTP 시스템의 고유값 CN_{TTP}를 생성하여 (5)DEC에 전송하고(5-1) DEM에도 식별자를 전송한다.

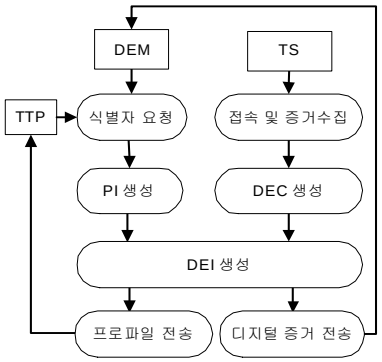
DEC는 (6) TS로부터 디지털 데이터를 수집하여 DEO (Digital Evidence Object)를 생성한다. 이후, 수집된 DEO와 저장된 CN을 이용하여 PI(Profile Info)를 생성하고, PI와 DEO를 결합하여 DEI(Digital Evidence Item)를 생성한다. 이때, PI는 디지털증거의 프로파일 정보로써

누가, 언제, 어디에서 생성되었는지에 대한 정보를 기록한다. 생성된 DEI는 (7) DEM에 전송되어 디지털증거로써 저장되고, PI는 (7-1) TTP에 전송되어 저장한다.

이후, DEM은 DEI를 이용하여보고서를 작성하여 법원에 제출하고, 프로파일을 이용하여 디지털증거의 무결성을 보증한다. 이때, 법원으로부터 프로파일의 무결성 확인요구가 발생하면, TTP에 저장된 PI값을 요청하여 프로파일의 무결성을 보증한다.

2. 디지털증거 수집 시스템

DEC는 DEM에 접수된 보안침해사고를 분석하기 위해 TS에 설치되고 해당 TS에 내포된 디지털 데이터를 분석하여 디지털증거를 수집한다. DEC의 기능은 디지털증거의 무결성 보증을 위해DEM 및 TTP로부터 식별자를 요청하고 수집된 식별자를 적용한 디지털증거의 프로파일을 생성하여 DEM 및 TTP로 전송한다.



<그림 3.3> DEC 구성도

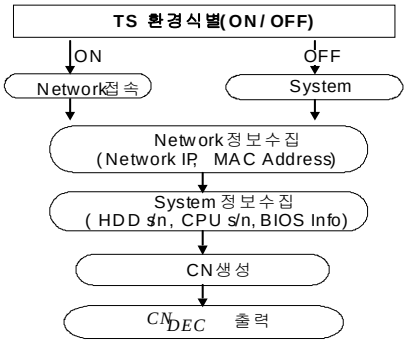
DEC는 다음과 같은 기능을 갖는다.

- 식별자 요청: TTP 및 DEM에 식별자 요청
- 증거수집: TS의 디지털 데이터를 읽어 디지털증거 수집
- 프로파일 생성: 수집된 디지털증거와 식별자를 적용한 디지털증거 프로파일 생성
- 프로파일 생성: 생성된 프로파일을 TTP에 전송
- 디지털증거 전송: 디지털증거 및 프로파일을 DEM에 전송

DEC와 TS, DEM, TTP의 세부운영 정책은 다음과 같다.

1) DEC와 TS

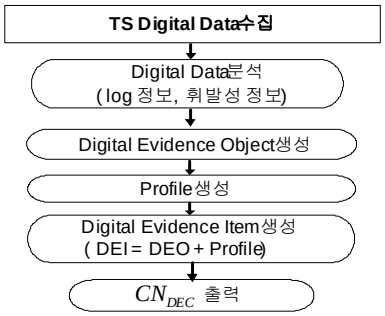
DEC와 TS는 TS의 환경에 따라 시스템정보를 획득하여 CN을 생성하고 생성된 CN은 TS를 식별하는 기능을 수행한다. 그리고 TS에 내포된 디지털 데이터를 분석하여 DEO를 생성한다. 그림 3.4는 TS와 DEC간의 CN 생성 절차를 보여준다.



<그림 3.4> CNDEC 생성

DEC는 TS에 접속하여 디지털 데이터를 분석한다. 이때, TS는 네트워크 연결이 가능한 On-line 환경과 Off-line 환경으로 분류할 수 있으며 각 환경에 따라 네트워크 접속 및 시스템에 직접 접속하여 정보를 수집한다.

수집 정보는 크게 네트워크 정보 및 시스템 정보로 분류할 수 있다. 네트워크 정보는 TS의 고유 MAC 주소 및 IP주소를 수집하고, 시스템 정보에서는 CPU 식별번호나 HDD S/N 및 BIOS 정보를 수집한다. 이후, 수집된 정보는 DEC에 의해 생성되는 DEO가 TS로부터 생성된 데이터라는 것을 보증하는 식별자로 사용된다. 그림 3.5는 DEC와 TS간의 DEO생성 절차를 보여준다.

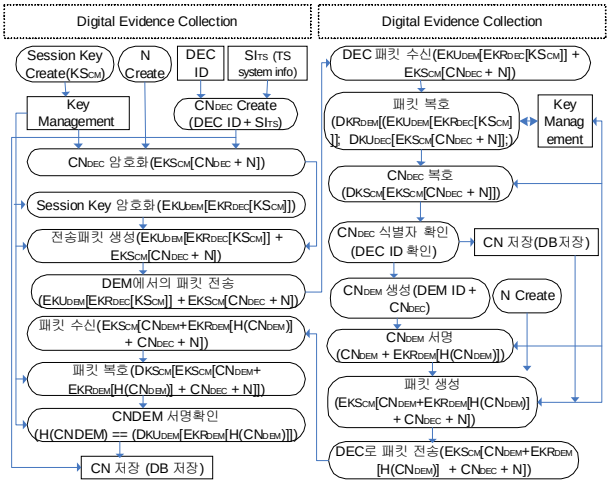


<그림 3.5> DEI 생성

DEC는 DEM 및 TTP로부터 프로파일에 필요한 식별자를 획득한다. 이후, TS에 접속하여 디지털 데이터를 수집, 분석하고 DEO를 생성한다. 생성된 DEO는 식별자를 이용하여 프로파일링을 수행하고, 그 결과로 DEI를 생성한다. 이때 PI는 디지털증거가 누가, 언제, 어디서, 무엇을 생성했는지에 대한 정보를 포함하고 있다.

2) DEC와 DEM

그림 3.6은 DEC와 DEM사이에 식별자 생성 절차를 보여준다.



<그림 3.6> DEC와 DEM 식별자 생성 절차

TS의 환경에 따라 시스템정보를 획득하여 CN_{DEC}을 생성하고(생성된 CN_{DEC}은 TS를 식별하는 기능을 수행) DEM으로 전송하여 확인한다. DEM은 CN_{DEC}값을 적용한 CN_{DEM}을 생성하여 안전하게 전송한다. 전송로 상의 보안을 위해 공개키기반의 인증서를 사용한다.

A. CNDEC 생성/전송

CN_{DEC}은 그림 [3.4]와 같이 생성되어 관용암호화 방식을 이용하여 전송한다.

▪ Packet = $EKU_{DEM}[EKR_{DEC}[KS_{CM}] + EKS_{CM}[CN_{DEC} + N]$

먼저 $EKU_{DEC}[EKR_{DEC}[KS_{CM}]]$를 이용하여 KS가 DEC로부터 DEM으로 안전하게 전송되었음을 보증할 수 있다. 또한, KS로 암호화된 $EKS_{CM}[CN_{DEC} + N]$는 기밀성을 보증할 수 있다. DEM은 자신의 개인키($DKR_{DEM}[EKU_{DEM}[EKR_{DEC}[KS_{CM}]]]$)와 DEC의 공개키($DKU_{DEC}$

[EKR_{DEC} [KS_{CM}]])로 KS를 획득하고, 암호문을 복호(DKS_{CM}[EKS_{CM} [CN_{DEC} + N]])하여 CN을 획득한다.

B. CNDEM 생성/전송

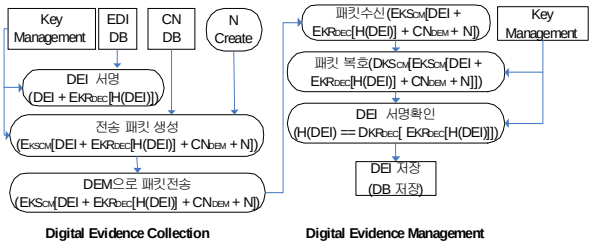
DEM은 CN_{DEC}를 적용하여 CN_{DEM}을 생성(DEM ID + CN_{DEC})하고 생성된 CN_{DEM}은 서명(CN_{DEM} + EKR_{DEM} [$H(CN_{DEM})$]) 되어 DEC에 전송된다.

▪ Packet = EKS_{CM}[CN_{DEM} + EKR_{DEM}[$H(CN_{DEM})$] + CN_{DEC} + N]

DEC는 서명 확인을 통해 CN_{DEM}을 확인한다.

C. DEI 전송/저장

그림 3.7은 DEI 전송 절차를 보여준다.



<그림 3.7> DEI 전송 절차

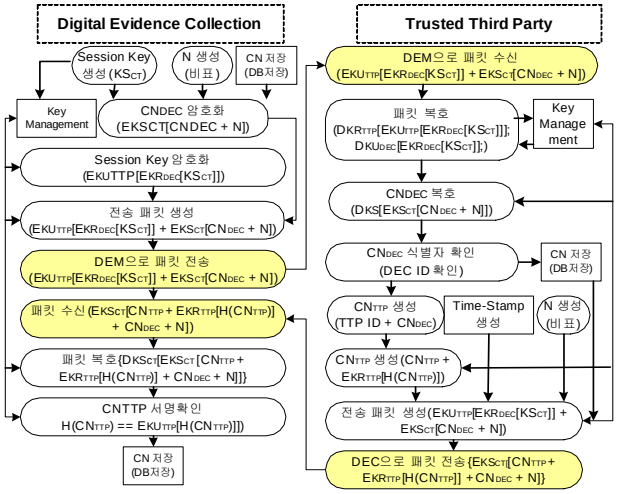
DEI DB에 저장된 DEI를 읽어 DEC의 개인키로 서명(DEI + EKR_{DEC}[H(DEI)])하여 DEM에 전송한다.

▪ Packet = EKS_{CM}[DEI + EKR_{DEC}[H(DEI)] + CN_{DEM} + N]

전송된 패킷은 KS로 복호하고(DKS_{CM}[EKS_{CM}[DEI + EKR_{DEC}[H(DEI)] + CN_{DEM} + N]]), 이후 DEI 서명을 확인(H(DEI) == DKU_{DEC}[EKR_{DEC}[H(DEI)]])한다. 확인된 DEI는 DB에 저장된다.

3) DEC와 TTP

그림 3.8은 DEC와 TTP사이의 식별자 생성 절차를 보여준다.



<그림 3.8> DEC와 TTP 식별자 생성절차

먼저, TS의 환경에 따라 시스템 정보를 획득하여 CN_{DEC}를 생성하고 TTP로 전송하여 확인하는 기능이다. 둘째로, TTP는 CN_{DEC}값을 적용한 CN_{TTP}를 생성하고 안전하게 전송하는 기능을 갖는다. 또한 전송로 상의 보안을 위해 공개키 기반의 인증서를 사용한다. 마지막으로 DEC는 PI를 TTP에 전송한다.

A. CNDEC 생성/전송

CN_{DEM}는 그림 3.4와 같이 생성되어 관용암호화 방식을 이용하여 전송한다.

▪ Packet = $EU_{TTP}[EKR_{DEC}[KS_{CT}]] + EKS_{CT}[CN_{DEC} + N]$

먼저, $EKU_{TTP}[EKR_{TTP}[KS_{CT}]]$를 이용하여 KS가 DEC로부터 TTP로 안전하게 전송되었음을 보증할 수 있다. 또한, KS로 암호화된 $EKS_{CT}[CN_{DEC} +N]$는 기밀성을 보증할 수 있다. TTP는 자신의 개인키($DKR_{TTP}[EKU_{TTP}[EKR_{DEC}[KS_{CT}]]]$) DEC의 공개키($DKU_{DEC}[EKR_{DEC}[KS_{CT}]]$로 KS를 획득하고 암호문을 복호($(DKS_{CT}[EKS_{CT}[CN_{DEC} + N]]$)하여 CN을 획득한다.

B. CNTTP 생성/전송

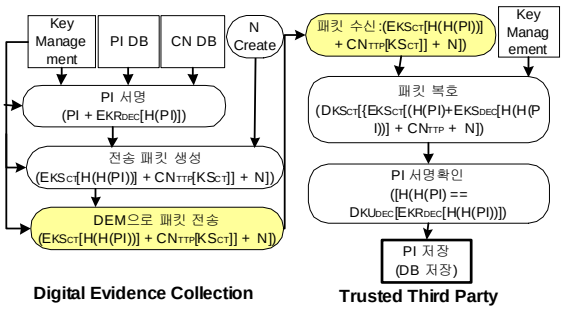
TTP는 CN_{DEC}를 적용하여 CN_{TTP}를 생성(TTP ID + CN_{DEC})하고 생성된 CN_{TTP}는 서명($CN_{TTP} + EKR_{TTP}[H(CN_{TTP})]$)되어 DEC에 전송된다.

▪ Packet = $EKS_{CT}[CN_{TTP} + EKR_{TTP}[H(CN_{TTP})] + CN_{DEC} + N]$

DEC는 서명 확인을 통해 CN_{TTP}를 확인한다.

C. PI 전송/저장

그림 3.9는 PI의 전송 절차를 보여준다.



<그림 3.9> PI 전송 절차

먼저, PI DB에 저장된 PI를 읽어 DEC의 개인키로 서명(H(PI) + EKR_{DEC}[H(H(PI))])하여 TTP에 전송한다.

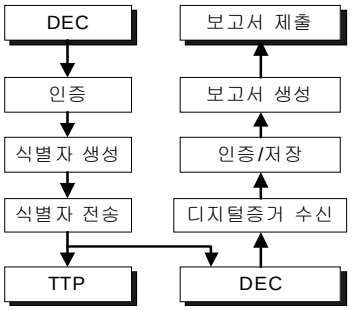
▪ Packet = EKS_{CT}[H(PI) + EKR_{DEC}[H(HPI)]] + CN_{TTP} + N]

전송된 패킷은 KS로 복호하고, 이후 PI 서명을 확인(H(PI) == DKR_{DEC}[EKR_{DEC}[H(H(PI))]])한다. 확인된 PI는 DB에 저장된다.

3. 디지털증거 관리 시스템

DEM의 기능은 크게 DEC 사용자 인증 및 디지털증거 저장, 증거제출 기능으로 분류할 수 있다. 먼저 DEC 사용자 인증은 DEM에 의해 DEC가 TS에 설치된다. 이때, DEC는 TS의 시스템정보를 이용하여 DEM에 정당한 권한을 가진사용자인지를 인증한다. 저장 기능은 DEC로부터 신뢰된 인터페이스를 통하여 디지털증거를 수신하고, 수신된 증거를 디지털증거 DB에 저장 관리한다. 즉, 시스템 정보를 취합하여 침해 근거가 되는 디지털증거의 프로파일을 보관한다. 그리고 저장된 디지털증거를 법원에 제출하기 위한 보고서 생성기능도 제공한다.

그림 3.10은 DEM의 구성을 나타내며 각시스템 구성요소의 기능은 다음과 같다.



<그림 3.10> DEM 구성도

- 인증: DEC가 정당한 사용자인지확인
- 식별자 생성: CNDEM 생성
- 식별자 전송: DEC에 식별자 전송
- 디지털증거 수신: DEC에 식별자 전송
- 인증/저장: 수신된 디지털증거와 프로파일에 대한 무결성 검증 및 검증된 데이터 디지털 증거 DB에 저장
- 보고서 생성: 디지털증거 DB로부터 디지털증거 생성, 법원 제출

이때, DEM과 TTP사이에는 CN에 대한 식별자 인증이 필요하다. 즉, DEC에 의해 생성되는 프로파일의 식별자를 확인하는기능을 제공한다.

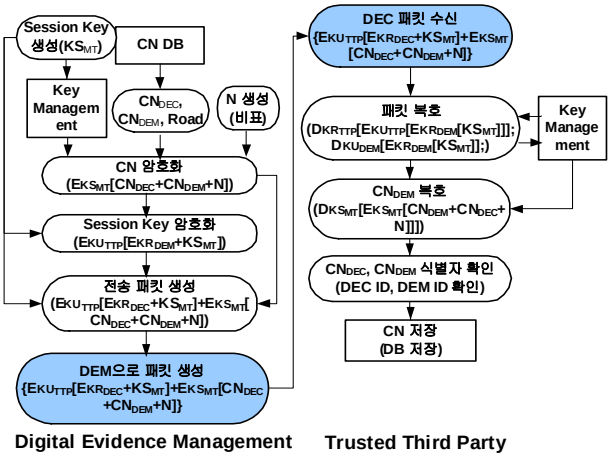
1) DEM 식별자 인증

DEM은 그림3.11에서와 같이 CN DB에서 CN_{DEC}, CN_{DEM}을 읽어 TTP에 전송한다.

▪ $Packet = EKU_{TTP}[EKR_{DEC}[KS_{MT}]] + EKS_{MT}[CN_{DEC} + CN_{DEM} + N]$

먼저, $EKU_{TTP}[EKR_{DEC}[KS_{MT}]]$를 이용하여 KS가 DEC로부터 TTP로 안전하게 전송되었음을 보증할 수 있다. 또한, KS로 암호화된 $EKS_{MT}[CN_{DEC} + CN_{DEM} + N]$는 기밀성을 보증할 수 있다.

TTP는 자신의 개인키($DKR_{TTP}[EKU_{TTP}[EKR_{DEC}[KS_{MT}]]]$)와 DEC의 공개키($DKU_{DEC}[EKR_{DEC}[KS_{MT}]]$)로 KS를 획득하고, 암호문을 복호($DKS_{MT}[EKS_{MT}[CN_{DEC} + CN_{DEM} + N]]$)하여 CN을 획득한다.



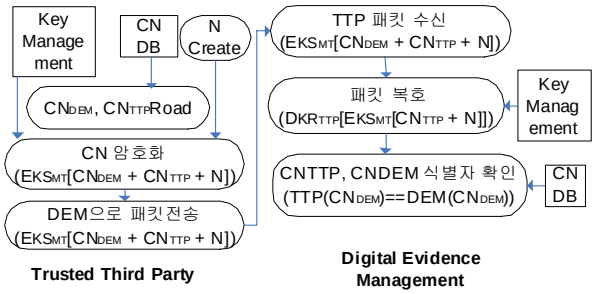
<그림 3.11> DEM 식별자 인증

2) TTP 식별자 인증

그림 3.12는 TTP 식별자 인증을 보인다. TTP는 CN DB에 저장된 CN_{DEM}, CN_{TTP}을 읽어 KS로 암호화하여 DEM에 전송한다.

▪ Packet = $EKS_{MT}[CN_{DEM} + CND_{TTP} + N]$

전송된 패킷은 KS로 복호($DKS_{MT}[EKS_{MT}[CN_{DEM}+ CN_{TTP} + N]]$)하고, 이후 DEM의 CN DB에 저장된 CN_{DEM}과 TTP로부터 수신된 CN_{DEM}을 확인한다.



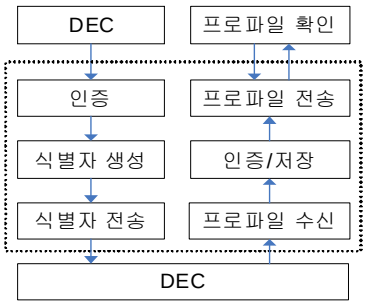
<그림 3.12> TTP 식별자 인증

4. 신뢰할 수 있는 제 3기관

TTP의 기능은 식별자 생성 및 전송, 프로파일 관리, TimeStamp 생성 기능으로 분류한다.

먼저 식별자 생성 기능은 디지털증거의 신뢰성 보증을 위해 CN_{DEC} 및 TT 등을 이용하여 생성한다. 프로파일 관리 기능은 DEC로부터 수신된 프로 파일 값을 프로파일 DB에 저장하고, 법원으로부터 디지털증거에 대한무결성 확인 요청시 프로파일을 전송한다. TimeStamp 생성 기능은 표준시간을 제공한다. 그림 3.13은 신뢰할 수 있는 제 3기관의 구성을 나타낸다. 각 시스템 구성요소의 기능은다음과 같다.

- 인증: DEC가 정당한 사용자인지 확인
- 식별자 생성: DS_{TTP} 및 TT 생성
- 식별자 전송: DEC에 식별자 전송
- 프로파일 수신: DEC로부터 프로파일 수신
- 인증/저장: 수신된 프로파일에 대한 무결성 검증 및 검증된 데이터 프로파일 DB 저장
- 프로파일 전송: 법원으로부터 디지털증거의 무결성 검증 요청이 있을 때 해당 프로파일 전송



<그림 3.13> TTP 구성도

TTP는 기관 내부에 설치할 수도 있지만 가능하면 DEM을 운영하는 기관에서 임의로 접근할 수 없는 기관에 설치하고 이에 대한 접근을 제한하는 명백한 정책이 필요하다.

5. 무결성 강화 보안 모델

1) IEB(Integrity Enforcement Blp)

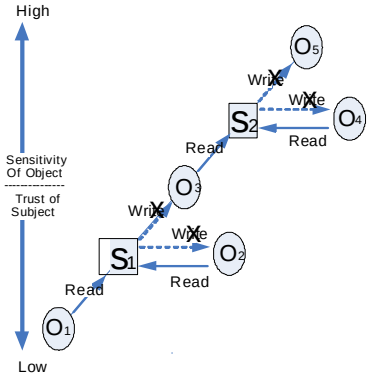
BLP 보안 모델에서 무결성을 위반하는 주요 원인은 하위 보안 등급의 주체가 상위 보안 등급의 객체에 쓰기를 허용하기 때문에 발생한다. 즉, 하위 보완 등급의 객체가 상위 보안 등급을 갖게 될 수 있으며 또한 의심스러운 주체가 고의적으로상위 보안 등급의 객체를 변경할 수 있는 허점이 있다. 따라서 하위 보안 등급의 주체는 상위 보안 등급의 객체에 쓰기를 금지한다

면 무결성을 유지할 수 있다.

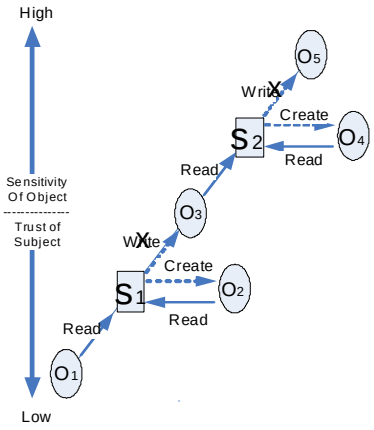
무결성 강화 보안 모델은 BLP 모델을 수정하여 비 신뢰적인 프로세스에 의한 중요 객체로의 접근을 차단하고, 프로세스의 악의적인 행위를 차단하기 위해 제안한모델이다. 제안된 IEB 모델은 컴퓨터 포렌식스 시스템 설계시 보안 모델로서 활용되며, 무결성 강화를 위해 정당한 권한을 갖는 주체는 새로운 객체에 대하여 읽기 및 새로운 생성만 가능하고 쓰고(변경)를 금지한다.

그림 3.14에서와 같이 같은 등급의 주체라 할여도 객체에 대한 쓰기 권한이 없고 단지 생성된 객체에 대한 읽기 권한만을 설정하여 객체에 대한 무결성을 강화하였다. 즉, BLP 보안 모델의단순 보안 성질은 그대로 유지하고 스타 보안 성질을 수정하여 쓰기보안 정책과 생성 보안 성질로 사용한다.

- 읽기 보안 성질: 주체 S는 객체 O를 C(s) >= C(o)일 경우 허가(S: 주체의 집합, O:객체의 집합, C(s):주체의 보안 등급, C(o): 객체의 보안 등급)



<그림 3.14> 무결성 강화 방안



[그림 3.15] 쓰기 성질의 제한

제안된 IEB 모델은 동급의 보안 등급을 갖는 주체라는 동급의 객체에 대하여 일기보안 성질만 갖고, 쓰기 보안 성질을 제한하지만, 컴퓨터 포렌식스 시스템에 있어 권한이 있는 주체는 새로운 객체를 생성하여 관리해야한다. 따라서 동급의 보안 등급의 쓰기를 허용하지만 동급의 보안 등급으로 새로운 파일을 생성하는 경우에만 쓰기를 허용하도록 해야 함으로서 다른 객체에쓰기가 아닌 생성에 따른 보안 성질을 따로 정의해야 한다.

그림 3.15와 같이 주체 S_1이 객체 O_1을읽어서 기존의 O_2에 쓰다면 무결성을 보장할 수 없지만 O_2라는 새로운 객체로 생성을 허용한다면 무결성을 보장할 수 있다. 따라서 같은 등급으로

의 쓰기기능을 생성만 허용하도록한다. 보안 성질을 정의하면 다음과 같다.

- 읽기 보안 성질: 주체 S는 객체 O를 C(s)>= C(o)일 경우 일기 허가
- 쓰기 보안 성질: 객체 O에 대해서 주체 S는 쓰기 금지
- 생성 보안 성질: 객체 O에 대해서 읽기 참조가 있는 주체 S는 C(s) = C(o)일 경우 새로운 객체 O에 생성 허가

(S: 주체의 집합, O:객체의 집합, C(s): 주체의 보안 등급, C(o): 객체의 보안 등급)

2) IEB 보안 규칙

A. 시스템 상태

- V = (B,M,F)는 시스템 상태의 집합
- B = S x O x A 는 접근 주체 S가 접근 개체 O를 A의 접근 동작으로 접근하는 것을 의미
- M: 접근 주체(사용자)가 접근 객체에 대해허가된 동작을 명시하는 접근행렬로서 행은 접근 주체를, 열은 접근 객체를 나타낸다. 단, M의 각 요소는 M[u, p]로 표시
- F = (fu, fc, fo,fp,fr): 주체/객체의 등급 검사 함수들(fu, fc, fo), 프로세스의 영역 검사 함수(fp) 및 동적 신뢰성 검사 함수(fr)
- fu: U →User Levels: 사용자의 최고 보안등급을 검사하는 함수
- fc: U →User Levels: 사용자의 현재 로그인등급을 검사하는 함수
- fo: O →Object Levels: 접근 객체의 보안등급을 검사하는 함수
- fp:PGE→{common, public}: 프로세스의 영역을 검사하는 함수

임의의 p ∈ PGE에 대해,

fp(p) = common, if p∈Common

fp(p) = public, if p ∈ Public

- fr:PGE ∈ C: 프로세스의 신뢰성을 검사하는 함수

B. 시스템

- System = (V, R, T, V_0)

시스템은 상태의 집합 V, 초기 상태인 V_0, 주체에게 객체에 대한 접근 권한을 부여하는 give access 및 부여된 권한을 제거하는 rescind access 같은 접근 요구의 집합 R, 그리고Transition function T:(V x R) → V로 구성된다.

C. 보안규칙

- ss-property
  If M[u,o] = r, then fc(u) >= fp(o)
- *-property
  If M[u,o] = a, then fo(o) = fc(u)
- ds-property
  If (s,o,a) ∈ B then a ∈ M[u,o]

이상과 같이 제안된 IEB 보안 모델은 컴퓨터 포렌식스 시스템 설계시 적용되어 컴퓨터 포렌식스 시스템의 신뢰성을 향상시키고, 이 시스템을 통해 생성된 디지털증거의 무결성 기능을 제공한다.

Ⅳ. 제안 메커니즘 평가

1. 평가 요구사항

피해 시스템, 가해 시스템, 경유 시스템 상에 존재하는 디지털증거 자체에대한 신뢰성, 디지털증거의 수집/보관에 대한 신뢰의 요구사항을 갖는다. 이러한 신뢰성 보증 서비스를 제공하는 제안 시스템은 디지털증거의 무결성 보증, 디지털증거의 객관화, 침입증거의 무결성 보증을 위한 접근통제의 평가 요구사항을 갖는다.

평가 요구사항을 각 항목별로 분석하여 제안 모델의 타당성을 제시하고기존 포렌식스와 비교 분석한다.

2. 디지털증거 무결성 보증 메커니즘 분석

1) 디지털증거의 무결성 보증

디지털증거의 무결성 보증은 디지털증거의 프로파일이 변경되지 않고 잘 보존되어 있다는 사실을 객관적으로 입증할 수 있어야 한다.

무결성을 입증해야하는 사용자는 디지털증거 프로파일 검증 메커니즘을 이용하여 검증할 수 있다. 즉, DEC에 의해 생성된 프로파일과 다지털증거는 각각TTP와 DEM에 안전하게 저장되어 있으므로, 저장된 프로파일 정보를 비교함으로써 디지털증거의 무결성을 입증한다.

먼저, DEM에 저장된 내용은 다음과 같다.

- DEM = DEI
- DEI = PI || DEO
- PI_{DEM}= CN_{DEC} || CN_{DEM} || CN_{TTP} || TT || H(DEO)

TTP에 저장된 내용은 다음과 같다.

▪ PI_{TTP} = H(CN_{DEC} || CN_{DEM} || CN_{TTP} || TT || H(DEO))

즉, DEM에는 DEC에서 수집된디지털증거에 대한 프로파일과 디지털증거를 보관하며, 디지털증거의 무결성은 PI를 통하여 증명한다. 그러나 DEM에 저장된 PI는 신뢰성에 대한 문제가 발생할 수 있으며, 이를 해결하기 위하여 DEC에 의해 TTP에 저장된 PI값을 요청하여 PI_{DEM} 값과 PI_{TTP} 값이 같음을 증명함으로 무결성을 보증한다.

▪ 무결성 보증 → if(H(PI_{DEM}) == PI_{TTP}) CDI

2) 디지털증거의 객관화

디지털증거와 관련한 기존 압수수색 방식에서는 매체에 의존하여 신뢰성을 보장하였다. 그러나 현재의 다중사용자 기반의 개방시스템환경에서는 압수수색으로 인한 가용성 서비스 및 제3자의 프라이버시 문제가 발생할 수 있다. 따라서 매체와는 독립하여 디지털증거 자체가 임의로 변경되지 않았다는 사실을 입증하는 매체 독립적 접근 방식이 필요하다.

매체 독립적 접근 방식에서는 수집되는 디지털증거를 객관화하여 프로파일을 생성한다. 프로파일은 생성자로부터 분리시켜 생성자가 이를 변경할 수 없다는 사실을 법과학적으로 증명할 수 있는 구조를 갖추어야 한다. 이러한 객관화의 방법에는 관리 주제의 객관화, 생성 시간의 객관화, 내용의 객관화, 기록방식의 객관화, 저장방식의 객관화 등을 이용한다.

A. 주체의 객관화

프로파일을 관리하는 주체를 생성자와 분리하고 생성자 이외의 주체로 하여금 프로파일을관리하게 하는 방식이다. 본 논문에서는 이를 위하여 생성자인 DEC와 관리자인 DEM 및 TTP를 이용한다.

- DEC: 디지털증거를 분석하여 DEI 생성
- DEM: DEI 관리
- TTP: PI 관리

즉, 생성되는 DEI를 생성자와 관리자로 분리하여 관리함으로써 주체를 객관화 시켰다.

B. 생성시간의 객관화

디지털증거를 생산한 시간과 프로파일을 생성한 시간을 확정함으로써 이후에 발생한 자료들과 구별하려는 노력이다. 디지털증거의 생산시기가 객관화됨으로써 이를 생산한 주체가 임의로 사후에 변경하지 못하게 하기 위한 방책이다.

▪ PI: CN_{DEC}|| CN_{DEM} || CN_{TTP}|| TT || H(DEO)

본 논문에서는 TTP에서 사건조사 및 증거 생성에 필요한 TimeStamp를 생성하여 객관화한다. TTP에서는 DEC로부터 식별자 요청시 식별자와 함께 TT를 제공한다.

C. 내용의 객관화

디지털증거의 내용을 더 이상 수정할 수 없도록 그 내용을 확정시키는 것으로 일반적으로 일방향 해쉬 함수가 이용된다.

▪ PI = CN_{DEC} || CN_{DEM}|| CN_{TTP} || TT || H(DEO)

PI는 DEO를 포함한 식별자를 이용하여 생성한다.

D. 기록방식과 저장방식의 객관화

디지털증거를 기록하여 저장할 경우에 이를 어떠한 이유로도 변경할 수 없도록 하기 위한 것이다. 기록방식에서는 첨가기록방식(Append-Only)을 사용하여 이미 기록된 디지털증거에 대해서는 고쳐 쓸 수 없도록 하는 방식을 말하고, 저장방식도 읽기전용방식(Read-Only)을 채택하는 방식을 사용하여 한번 기록된 디지털증거가 다시 변경되는 일이 없도록 통제하는 방식이다.

본 논문에서는 IEB 보안모델의 보안성질을 이용하여 제공한다. 즉, 권한이 있는 주체는 새로운 객체를 생성할 수 있지만 수정할 수 없다.

3) 침입증거의 무결성 보증을 위한 접근통제

피해시스템의 침입정보가 포렌식스 증거로 효용성을 발휘하기위해서는 증거물의 원본 보호 무결성 기능을 제공해야 한다. 즉, 침입 흔적이 법적으로 효용성을 제공하기 위해서는 변경되거나 삭제로부터 보호되어야 한다. 시스템을 사용하는 주체에 따라 보안 보안 등급이 설정되고

자신의 보안 등급보다 높은 개체는 접근을 할 수 없다.

그러나 접근이 허용된 개체라도 포렌식스 정보로 활용되기 위해서는 등급과는 별개로 쓰기 및 수정으로부터 보호되어야 한다. 또한 같은 개체가 존재할 때, 새로이 생성되는 개체는 기존 개체에 겹쳐 쓰지 못하도록 보호해야 한다. 주체의 집합(S), 개체의 집합(O), 주체의 보안등급(C(s)), 개체의 보안 등급(C(o))은 침입 증거를보호하기 위하여 다음과 같은 보안 정책을 갖는다.

- 읽기 보안 성질: 주체 S는 객체 O를 C(s) >= C(o)일 경우 일기 허가
- 쓰기 보안 성질: 객체 O에 대해서 주체 S는 쓰기 금지
- 생성 보안 성질: 객체 O에 대해서 읽기 참조가 있는주체 S는 C(s) = C(o)일 경우, 새로운 객체O에 생성 허가

(S: 주체의 집합, O: 주체의 보안 등급, C(s): 주체의보안 등급, (Co): 객체의 보안 등급)

3. 디지털증거 무결성 보증 메커니즘 평가

제안된 디지털증거 무결성 보증 모델의 평가는 4.1에서 도출된 요구사항을 바탕으로 기존 포렌식스 시스템과 비교하여 평가하였다. 제안된 방식은 디지털증거에 대한 프로파일을 생성하여 누가, 언제, 어디서, 무엇을 했는가에 대한 정보를 포함하며, 이것은 대상시스템으로부터 디지털증거에 대한 매체 독립적 분석을 가능하게 하였다. 이것은 대상시스템으로부터 디지털증거에 대한 매체 독립적 분석을 가능하게 하였다. 수집된 디지털증거는 TTP에 저장된 프로파일에 의해 무결성을 제공한다.

평가 요구사항을 각 항목별로 분석하여 제안 모델의 타당성을 기존 포렌식스와 비교하여 제시하며 각 평가 항목은 다음과 같다.

- 컴퓨터 포렌식스 도구의 신뢰성
- 디지털증거의 무결성 보증
- 가용성 서비스
- 디지털증거의 객관화

표 4.1은 기존 컴퓨터포렌식스 시스템과 제안된 디지털증거 무결성 보증 모델을 평가하였다.

<표 4.1>

요구사항	기존방식	제안방식	비고
시스템 자체의 신뢰성 검증	X	Δ	TTP 이용
컴퓨터 포렌식스 도구의 신뢰성 검증	Δ	O	TTP 이용
가용성 서비스 제공	X	O	매체독립적
디지털증거의 무결성 서비스 제공	Δ	O	디지털증거의 객관화
주체의 객관화	X	O	직무분리
생성시간의 객관화	X	O	TTP의 TImeStamp 이용
내용의 객관화	O	O	Hash 함수
기록방식의 객관화	Δ	O	IEB 적용
저장방식의 객관화	Δ	O	IEB 적용

(O: 지원, Δ:부분적 지원, X:지원하지 않음)

기존방식의 경우, 시스템 및 프로그램의 신뢰성을 검증할 수 있는 메커니즘은 없다. 단지, 몇몇의 프로그램의 경우 개발업체가 자체적으로 기준값을 만들어 제공한다. 제안방식에서는 프로그램을 처음 설치에서부터 현재까지의 상태정보를 신뢰된 관리자에 의해 프로파일링 되고, TTP에 저장하여 프로그램의 신뢰성을 제공한다.

디지털증거의 무결성 보증의 경우, 기존방식은 대상시스템 및 자원의 압수수색을 원칙으로 하여 압수된 원본 데이터와 디지털증거가 같음을 증명함으로써 무결성을 제공한다. 제안된 방식의 경우, 매체 독립적 방식으로 가용성을 제공하면서 디지털증거를 수집할 수 있다. 디지털증거의 신뢰성을 보증하기 위해 프로파일을 생성하고, 생성된 프로파일을 TTP에 저장되어 디지털증거의 무결성 보증을 위해 사용된다.

침입증거의 무결성 보증을 위한 접근통제의 경우, 기존방식에서는 일반적 접근통제 모델을 사용함으로 수정이 불가피하다. 제안된 방식의 경우 제안된 IEB 모델을 사용하여 정당한 권한을 가진 사용자의 불법적 변형을 제한할 수 있다.

제안된 방식에서는 디지털증거 생성을 위한 DEC와 관리를 위한 DEM 그리고 검증을 위한 TTP로 구성되어 생성과 관리의 권한을 분리 하였다. 또한, TTP를 통해 사건처리의 표준시간을 제공함으로써 생성시간의 객관화 및 프로파일링을 통해 내용의 객관화를 제공하였다. 즉, 제안된 디지털증거 무결성 보증 메커니즘은 기존 시스템 환경에서 매체 독립성을 적용하여 가용성 서비스를 제공하였으며 대상 시스템에서 수집, 생성된 디지털증거를 객관화함으로써 신뢰성을 보증한다.

Ⅴ. 결론

본 논문에서는 스마트홈 환경에서 발생할 수 있는 시스템 오류 및 침해의 원인을 파악하고 범죄행위에 대한 법적대응 증거자료를 보호함으로써, 증거자료의 신뢰성을 높이기 위하여 디지털증거의 매체 독립적인 속성을 이용한 디지털증거 보증 메커니즘을 제안하였다.

제안한 메커니즘은 스마트홈 환경에서 발생하는 범죄에 대한 수사절차와 침해사고 대응과정에서 획득되는 디지털증거의 신뢰성을 향상시켜 사법정의 실현과 정보보안 강화에 기여할 수 있다. 더 나아가 범죄가 발생하기 이전에 사건 발생에 대비하여 시스템과 주요 프로그램에 대한 무결성 검증의 기준점 마련과 사건발생 이후에 시스템과 주요 프로그램에 대한 침해사실을 확인하기 위한 목적으로 운용될 수 있다. 또한 디지털 자료처리의 전반적 분야에 적용함으로써 중요한 전자적 거래에 있어서 신뢰성을 보증하기위한 인프라로 발전시켜 전자적 거래의 안전에 기여하는데 활용될 수 있다.

향후, 제안한 디지털증거의 무결성 보증 메커니즘이 실무현장에서 널리 이용되기 위해서는 정보차원의 신뢰기관 구축을 필요로 한다. 또한 디지털증거를 생성하고 처리 운영하는 대상시스템 및 주요프로그램에대한 신뢰성 보증을 위한 체계적인 연구가 필요하다.

참고문헌

[1] Warren G. Kruse ii, Jay G. Heiser, “COMPUTER FORENSICS: Incident Response Essentials,″ Addison Wesley.

[2] Gray Palner, *A Road Map for Digital Forensics Research. Technical Report DTR-T001-01.* DFRWS. November 2001. Report From the Fiest Digital Forensic Reserch Workshop(DFWS)

[3] Michael A. Caloyannides, “Computer Forensics and Privacy,″ Artech House, 2001.

[4] Eoghan Casey, “Handbook of Computer Crime Investigation: Forensic Tools & Technology”, 2001.

[5] Albert J. Marcella Jr (Editor S. Greenfield, “Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes,″ 2002.

[6] Lee Garber, “Encase: A Case Study in Computer-Forensic Rechnology,″ *IEEE Computer Magazine* Jan. 2001.

[7] *TCT: The Coroner's Toolkit,* http://www.fish.com/tct

[8] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, “Role-

Based Access Control Models," *IEEE Computer, vol.29,* 1996.

[9] Shon Harris, "CISSP Certification Exam Guide," McGraw Hill, 2003.

[10] David F. Ferraiolo, Janet A. Cugini, and D. Richard Kuhn, "Role-Based Access Control (RBAC): Features and Motivations," 11th Annual Computer Security Application Conference, Dec 1995.