Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.781

보안 저장장치를 구비한 가상의 인비저블한 보안 디스크 (VIPDISK) 설계 및 구현

전 선 국,[1†] 권 용 구[2‡]
[1]중국 연변대학 과학기술학원, [2]필립소프트웨어

Design and Implementation of Virtual and Invisible Private Disk (VIPDISK) having Secure Storage Device

Shan Guo Quan,[1†] Yong-Gu Kwon[2‡]
[1]YanBian University of Science and Technology, China, [2]Philipsoft, Korea

요 약

본 논문에서는 정보유출을 막기 위하여 보안저장장치를 구비한 가상의 인비저블한 디스크(VIPDISK)기술을 제안한다. 제안 기술은 소프트웨어 기반의 보안 기술로서, 임의의 데이터 저장장치의 운영체제에서는 전혀 확인 할 수 없는 숨은 보안 영역을 설정하여 해당 영역에서 OS를 포함한 어떤 프로그램을 실행하더라도 보안영역의 존재여부를 전혀 알 수 없게 한다. 특히 비활성화상태에서는 타인에게 절대 노출되지 않는 보안 영역을 설정하여 고유의 디지털 키와 복호화 툴을 여는 사용자 암호에 의해서만 활성화되어 사용 가능하게 된다. 그리고 숨은 보안영역에 저장되는 모든 데이터는 실시간으로 암호화하여 저장되므로 만약 VIPDISK가 분실하거나 도난당해도 보안 영역에 저장된 데이터가 절대 유출되지 않도록 보호해준다. 실험을 통하여 VIPDISK는 기존 기법들에 비해 높은 보안성을 제공하는 것을 알 수 있었다.

ABSTRACT

This paper proposes a virtual and invisible private disk (VIPDISK) technology equipped with the secure storage devices. As a software based security technology, it can create hidden partitions on any data storage device which can not be identified by the windows OS, so the program running on it, does not have any evidence of the existence of the hidden storage space. Under inactive state, it maintains an unexposed secure partition which can only be activated with a matching combination of a unique digital key and a user password to open the decryption tool. In addition, VIPDISK can store data to secure storage device with real-time encryption, it is worry-free even in the case of lost or theft. Simulation results show that VIPDISK provides a much higher level of security compared to other existing schemes.

Keywords: Secure storage device, virtual, hidden storage space, digital key, activated, inactivation, decryption tool

I. 서 론

최근 노트북, 태블릿 PC, 데스크 탑 PC, 스마트폰 등 다양한 컴퓨터들의 보급이 일반화되고 클라우드 컴퓨팅 환경의 구축됨에 따라 대부분 사용자들은 중요 정보들을 컴퓨터나 이동형 저장장치(i.e. USB, 이동HDD 등) 및 클라우드에 저장하여 사용하고 있다. 하지만 컴퓨터에 중요한 정보를 저장하여 관리하고, 클라우드 컴퓨팅 환경을 이용하는 것은 언제 어디서나 누군가에 의해서 자신이 사용하고 있는

접수일(2015년 2월 13일), 수정일(2015년 7월 27일), 게재확정일(2015년 8월 1일)
† 주저자, sgquan@yust.edu
‡ 교신저자, philip@philipsoft.co.kr(Corresponding author)

컴퓨터가 해킹될 수 있는 환경을 제공하며, 해커 또는 주변의 다른 사람들에게 의해 컴퓨터에 저장되어 있는 개인의 중요한 정보가 쉽게 유출될 수 있는 위험요소들이 존재한다[1-3]. 그리고 중요한 자료를 저장하고 있는 이동형 저장장치들은 분실되거나 부주의로 잘 보관되지 않았을 경우에는 누군가에 의해 개인 정보가 분실, 유출되는 피해까지 따라 온다. 때문에 많은 사용자들은 자신만의 사용 가능한 저장 공간에 저장된 데이터들을 안전하게 보호하고 편리하게 관리할 수 있는 보안 기법을 필요하고 있다. 하지만 기존 대부분 보안 기법들은 저장 디스크로부터 데이터 이동을 차단하거나 감시하는데 치중되어 있기에 상대적으로 쉽게 무력화된다. 이러한 문제점 해결을 위하여 최근 많이 사용되는 방법은 보안저장장치를 적용한 기법들인데 현재 다양한 보안 시스템들에 적용되고 있다[4-13].

그 가운데서도 가장 쉬운 기법은 컴퓨터 부팅 시 아이디와 비밀번호를 입력하는 로그인 방식의 보안 시스템이다. 아이디 및 비밀번호의 입력만으로 하는 암호화 기법은 일단 아이디 및 비밀번호가 노출되면 컴퓨터의 모든 정보가 유출될 수 있는 문제점들이 존재한다. 그 외에도 부분 파일과 디렉터리를 암호화하는 방법도 있지만 이런 방법의 보안 취약점이 알려지면서 중요한 데이터는 가상볼륨을 사용하여 일반 영역과 분리를 시켜서 보호하는 기술[4,5]들이 있다.

[6]에서는 윈도우 응용 프로그램을 위한 하이퍼바이저(Hypervisor)가상화 기술을 이용한 가상화 컨테이너를 구성하여 응용프로그램 격리를 통해 개인정보를 보호하는 보안 솔루션과 융합한 보안 컨테이너 클라이언트를 구성한다. Linux 전용 솔루션인 Docker[7,8]를 이용하여 Linux 전용으로 컨테이너 기술을 똑같이 적용될 수 있다. 하지만 [6]과 정보 유출 방지를 위해 Docker를 이용한 보안 컨테이너는 모두 운영체제에 의존성이 높은 기술이기 때문에 OS에서 유발되는 다양한 보안 취약점으로 인해 여전히 발생되는 정보유출의 많은 취약점도 그대로 가지고 있다.

그 외에 하드디스크 전체를 암호화하는 Full Disk Encryption(FDE)방법[9]이 있는데 이는 접근을 위한 패스워드와 토큰이 없다면 디스크 사용이 불가능함은 물론이고 강제로 시스템에 마운트 하더라도 암호화된 데이터만 노출되게 하고 있다. FDE 기반의 데이터 보호 방법은 크게 소프트웨어 방식과 하드웨어 방식을 사용한 방법으로 나뉘는데 그중에 소프트웨어 방식을 사용한 보안저장장치는 인증을 통한 루틴이나 정보들이 쉽게 노출될 수 있고 하드웨어 방식은 정보들을 잘 숨길 수 있지만 사용편의성이나 이동성 면에서 소프트웨어 비해 떨어지기 때문에 소프트웨어를 많이 사용한다[10]. 하드웨어를 사용하는 보안저장장치는 소프트웨어보다 접근할 수 있는 방법이 제한되었기에 비교적 안전하다고 생각하지만 실제 취약성 분석 결과로는 잘 설계된 소프트웨어 보안 제품은 매우 안전한 성능을 가짐을 알 수 있다. 이 관점을 기초로 제안 기법도 소프트웨어 기반으로 구성한다. [11]에서는 컴퓨터의 저장장치 전체 또는 저장장치의 일부 영역을 암호화하거나 선택된 특정 파일만을 암호화하고, 특정 인증절차를 통해서만 설정된 일부 영역 또는 파일을 사용할 수 있도록 하는 암호화 방식의 저장장치 보안 시스템이 있다. 하지만 이런 기법들은 아이디와 비밀번호를 모르더라도 저장장치에 암호화된 별도의 영역이 있음을 알 수 있어 해커 등에 의한 전문가 임의의 영역에 대한 아이디와 비밀번호의 해킹 시도를 유발시킬 수 있고 이로 인해 정보가 유출되는 문제점이 존재한다.

[12]에서는 일부 권한을 가진 관리자의 액세스 권한을 제한하여 사생활 정보를 보호하기 위해 스마트폰에 장착된 물리적 디스크에 논리적인 디스크인 가상 디스크를 새롭게 생성하여 일반 공개 파일은 기존처럼 물리적 디스크에 저장하여 관리하고 개인 프라이버시 파일은 논리적인 디스크인 가상 디스크에 저장하여 보안을 강화한다. 하지만 이런 기법은 기존의 MDM(Mobile Device Management)솔루션을 적용하는 단점과 함께 여전히 운영체제에 의존한 보안 기술이다.

위에서 언급된 대부분 기법들은 OS개론에서 언급된 일반적인 디스크 관리 이론 즉 윈도우, 리눅스를 포함한 거의 모든 OS에서 이미 파티션, 볼륨 등의 소위 매핑 테이블에 기초하여 디스크를 관리하고 있다. 그렇다 보니 실제 디스크 사용자의 관점에서는 자신이 사용하는 OS에서 제공하는 쉘(Shell)에서 제공하는 드라이브, 폴더, 파일의 형태로만 디스크를 이용할 수밖에 없는 단점이 있다. 쉘에서 제공하는 드라이브, 폴더, 파일에 대한 각종 보안솔루션은 물론 OS자체적으로도 이미 암호화라는 기법을 제공하고 있지만, 결국 파티션 및 볼륨으로 구성되는 특정 영역에 존재하는 폴더나 파일 자체의 존재정보까지는 보호할 수 없는 한계가 있다.

본 논문에서 제안 기술은 운영시스템에 무관하게

모든 저장디스크를 직접 제어하는 물리적 보안 기술로서 기존의 운영체제이론에서 전혀 존재하지 않는 독자적인 새로운 논리구조를 이용하여 디스크 전 영역을 자유롭게 제어할 수 있도록 한다. 즉 컴퓨터의 저장 시스템이 비활성화상태에서는 운영시스템의 어플리케이션을 통해서는 보안 저장 영역의 존재 여부를 전혀 알 수 없고 디지털 키(AES256으로 암호화)를 포함하는 어플리케이션을 통한 사용자의 비밀번호를 입력 시 해당 디지털 키와 비밀번호에 의해서만 활성화되어 사용할 수 있는 보안 디스크 영역을 포함하는 저장 시스템 및 방법이다. 또한 외부에서 해커가 침입하거나 PC나 스마트폰 등 데이터 저장 기기들이 분실, 도난당해도 중요 문서가 있는지 알 수 없게 하는 솔루션이다. 외부에서 볼 때 파일이나 프로그램 검색기로 찾거나 숨긴 파일을 보이게 해도 보안 디스크 안에 있는 정보는 나타나지 않게 한다.

II. 제안 기술: VIPDISK

VIPDISK기술은 OS와 무관하게 컴퓨터에서 인식 가능한 모든 디스크를 직접 제어하는 기술이다. 즉 일반적인 OS개론에서 사용하는 일반적인 디스크 관리 이론과 전혀 무관한 방법으로 디스크를 제어하여 궁극적으로 보안 특성의 이점을 얻고자 하는 컨셉의 기술로 개발되었다. 기존의 모든 보안솔루션은 기존 OS의 쉘의구조에 상당한 의존성을 갖고 있다.

VIPDISK 기술은 이러한 고전적인 파티션, 볼륨정보 등등의 Mapping Table에 기반한 디스크 관리정보를 전혀 사용하지 않고 독자적인 Digital Key(AES256으로 암호화)라는 새로운 논리구조를 구성하고 이를 통해 디스크의 전 영역을 원하는 만큼의 크기와 별도의 영역으로 나누어 자유롭게 제어할 수 있도록 한다. 단 여전히 사용자는 OS가 제공하는 Shell에 익숙하므로 정상적인 인증을 득한 경우에만 VIPDISK내에 데이터를 일반적인 드라이브, 폴더 및 파일의 형태로 제공한다. 필요에 의해서는 기존의 쉘 구조를 굳이 유지하지 않고 상위레벨의 응용프로그램에서 독자적으로 I/O로서 제공할 수 있다. 정상적인 인증을 거친 상태에서 VIPDISK에 관리되는 디스크의 물리적인 공간에 저장되는 모든 데이터는 자동으로 암호화(현재 SEED128 사용)하고 사용자가 해당 파일을 열람하는 등의 이유로 읽기가 발생되면 역으로 자동적으로 복호화 하도록 고안되었다. 실제 VIPDISK영역에 저장된 데이터는 궁극적으로 기존의 파티션 및 볼륨 등의 매핑 테이블 내 그 어떠한 정보도 없게 되며 실제 저장되어 있는 RAW 데이터조차도 암호화 되어 있으므로 기존의 모든 OS에서 정상적으로 VIPDISK자체의 인증을 받기 전까지는 어느 누구도 VIPDISK 보안 구역 존재는 물론 그 데이터의 해석도 불가능하게 되는 보안 특성을 제공하는 구조가 된다. 즉 다시 말하면 VIPDISK는 기존의 운영체제 이론에 전혀 존재하지 않는 새로운 디스크 관리기법을 제시하고 이를 통해 기존의 상용화된 모든 OS가 전혀 정상적인 VIPDISK자체의 인증 없이는 인식조차 할 수 없도록 하기 때문에 기존의 OS에서 유발되는 다양한 취약점에 의해 발생되는 정보유출의 원천적인 차단이 가능한 장점이 있다. VIPDISK 기술에서 가장 중요한 것은 각 보안 디스크영역이 생성될 때마다 고유하게 생성되는 디지털 키라는 512바이트의 정보이다. 이는 어플리케이션의 구조 또는 사용 환경에 따라 어플리케이션 내에 리소스로도 포함할 수 있고 필요시 디지털 키만을 따로 관리하는 서버를 두고 그 내부에 저장한 후 다양한 사용자 인증체계를 통해 선별적으로 이용하여 설정된 보안 디스크 영역을 제어하는 모델도 가능하다.

III. VIPDISK 구성 및 동작관리

본 장에서 VIPDISK의 구조 설명과 함께 VIPDISK의 동작 및 관리 방법을 설명한다.

3.1 VIPDISK 시스템 구성

Fig.1.과 같이 VIPDISK 시스템은 크게 어플리케이션 계층, 커널 계층, 저장 장치 그리고 보안디스크 어플리케이션 등 4개 부분으로 구성된다.

◉ 저장 장치:

저장 장치는 임의의 용량을 가지고, 일반 데이터들을 저장하는 일반 영역으로 구성된 일반 디스크와 디지털 키가 저장되는 디지털 키 영역과 디지털 키로 의해 암호화되는 보안 데이터 영역 구비하는 보안디스크를 포함한다. 저장 장치의 보안 디스크 영역은 미할당 영역으로 파티션 되는 것이 특징이다. 디지털 키 영역은 Fig.2.와 같이 임의의 크기로 결정될 수 있으며 디지털 영역에 저장되는 디지털 키는 하나의 원본 디지털 키로 구성되거나 혹은 원본 디지털 키를

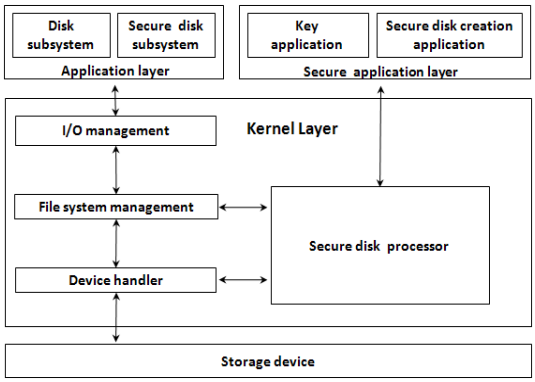

Fig. 1. VIPDISK system architecture

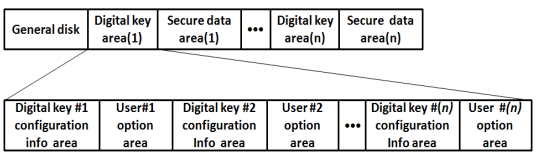

Fig. 2. VIPDISK data storage structure

복제한 적어도 하나 이상의 복제 키들로 구성된다.

원본 디지털 키와 복제 디지털 키는 시작섹터 정보가 동일하고, 마지막 복제 디지털의 섹터 오프셋 정보만 다르게 하거나 혹은 원본 디지털 키 및 복제 디지털 키들의 섹터 오프셋들 각각 서로 상이하게 구성된다.

복수의 각 디지털 키의 시작 섹터 정보는 랜덤하게 구성한다. 그 외는 포함된 암호화키, 디스크볼륨 이름, 비밀번호, 파괴키, 디스크 일련번호, 시작섹터 번호, 보안 디스크 크기, 자동 잠금 여부 설정, 섹터 오프셋 정보 및 보안 디스크 타입 등 다른 정보들은 동일하게 구성된다.

◉ 어플리케이션 계층:

운영시스템의 사용자 모드 혹은 어플리케이션 계층에서 실행되는 어플리케이션으로 윈도우즈, 리눅스, 맥, 유닉스, 안드로이드 또는 iOS등의 운영시스템의 탐색기 또는 쉘 프로그램 등이 된다. 어플리케이션 계층에서 디스크 서브시스템은 어플리케이션 계층의 구동과 함께 구동되어 커널 계층를 통해 폴더 및 파일 등의 일반 데이터를 저장 장치에 저장하고, 저장되어 있는 일반 데이터들을 읽어 표시하는 등의 처리를 수행한다. 한편으로 보안디스크 서브시스템은 열쇠 어플리케이션에 의해 생성된 저장 장치의 보안디스크에 대한 입출력을 처리한다. 보안디스크 서브시스템은 활성화된 보안디스크에 대해 데이터 입출력 발생 시 보안디스크 처리기를 통해 데이터들을 암호화하여 보안 디스크에 저장하고, 저장된 암호화 데이터를 읽어 들여 복호화 한다.

◉ 열쇠 어플리케이션:

열쇠 어플리케이션 실행 시 아이디와 패스워드를 입력시 활성화 되면, 보안설정 해제 모드에서 저장 장치의 보안디스크를 활성화시키고 어플리케이션 계층에 보안 디스크 서비스 시스템을 마운트 시킨다. 열쇠 어플리케이션은 보안디스크 비활성화 이벤트 발생 시 어플리케이션 계층으로부터 보안 디스크 서브시스템을 언 마운트 시킨다. 보안 디스크 비활성화 이벤트는 열쇠 어플리케이션의 활성화시 활성화된 사용자 인터페이스 수단에 의한 열쇠 어플리케이션의 정상적인 종료 또는 강제적인 종료에 의한 열쇠 어플리케이션 종료 이벤트가 될 수 있고 보안디스크를 포함하는 저장장치의 분리에 의해 발생되는 저장장치 분리 이벤트가 될 수도 있다.

Fig.3.과 같이 열쇠 어플리케이션은 서비스 실행부, 서비스 실행 제어기, 디지털키 보관소 및 서비스 실행 감시로 구성된다. 디지털키 보관소는 저장 장치의 보안디스크의 디지털 키 영역에 저장된 디지털 키(사용자 옵션 정보는 제외)와 동일한 디지털 키를 저장한다. 서비스 실행부는 보안저장장치를 구비하는 저장 시스템의 전반적인 동작을 제어한다. 특히 서비스 실행 부는 사용자 옵션정보 설정, 저장 장치의 보안설정해제 및 보안 설정 수단을 포함하는 사용자 인터페이스 수단을 표시한다. 입력 처리는 사용자 인터페이스 수단에 대응하는 입력을 수신 받아 서비스 실행 제어기로 출력한다. 서비스 실행 제어기는 열쇠 어플리케이션의 실행시 커널 계층에 보안 디스크 처리기를

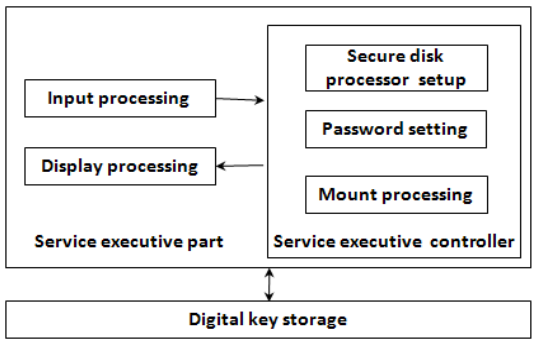

Fig. 3. Key application structure

생성하는 보안디스크 처리기 설치, 디스플레이 처리를 통해 제공되는 사용자 인터페이스 수단을 통해 사용자 암호 설정 수단을 제공하고, 사용자 암호 설정 수단을 통해 사용자 암호를 등록하거나 변경하여 디지털키 보관소 또는 저장 장치의 디지털키 영역의 디지털 키의 사용자 옵션 영역에 저장하는 암호 설정부 및 입력 처리를 통해 보안디스크 즉 보안디스크 서브시스템이 어플리케이션에 마운트 되거나 마운트 해제되도록 하고 마운트 된 경우 어플리케이션에 의해 저장 장치의 보안디스크에 대한 데이터 처리 입출력이 발생할 때 커널계층의 보안디스크 처리기에 의해 데이터를 처리를 수행하도록 하고, 마운트가 해제된 경우에는 이를 중지시키도록 하는 마운트 처리기를 포함한다. 서비스 실행 감시는 실행부의 동작 상태를 감시하여 서비스 실행부의 강제 종료 이벤트를 검출시 보안디스크를 닫는다. 즉 서비스 실행 감시부는 서비스 실행부의 강제 종료 시 보안설정해제 모드에서 보안 설정모드로 전환하여 보안디스크를 활성화시킨다. 이는 해커가 서비스 실행부를 강제 종료시킨 후, 활성화되어 있는 보안 디스크로부터 데이터를 빼내어 가는 것을 방지하기 위한 것이다. 서비스 실행부 강제 종료 이벤트는 서비스 실행부의 동작 종료 및 보안 디스크를 포함하는 저장 장치를 분리 시에 발생 될 수 있는 것이다.

◉ 커널 계층:

어플리케이션에서 발생되는 입출력 요청들에 대응하여 저장 장치에 저장할 데이터 및 저장된 데이터들의 입출력 처리를 수행한다. 커널 계층에서 입출력관리, 파일 시스템 처리, 디바이스 처리가 포함되는데 이미 윈도우환경에서 잘 알려져 있는 기술이므로 그 상세한 설명은 생략한다. 디바이스 처리기는 파일 처리에서 요청된 데이터 처리 요청에 대해 물리적인 저장 장치를 제어하여 해당 데이터에 대한 처리를 수행하고, 그 결과를 파일 시스템 처리로 리턴 한다. 그리고 열쇠 어플리케이션이 활성화됨과 동시에 이로 인해 커널 계층에는 보안 디스크 처리기가 생성된다. 생성된 보안디스크 처리기는 열쇠 어플리케이션의 제어를 받아 보안 디스크를 포함하는 저장 장치를 검출하며, 보안설정해제 모드에서 보안디스크를 어플리케이션부에 마운트 된 보안디스크 서브시스템으로부터 데이터 입출력에 따르는 입출력을 요청을 받고, 입력된 입출력 요청들을 처리하기 위한 객체들을 생성한다. 또한 보안 디스크 처리기는 보안 서브시스템에서 발생된 요청들에 대응하는 검출된 보안디스크에 저장할 데이터 및 저장된 데이터들에 대한 입출력 요청을 입출력 관리 및 파일 시스템 처리를 통해 입력받고, 입출력 요청에 대응하는 처리를 수행한 그 처리 결과를 파일시스템 처리를 통해 저장 장치의 보안 디스크에 해당 입출력 요청에 대한 처리를 수행한다. 보안디스크 처리기는 디바이스 처리기로 요청에 대한 데이터를 제공시 암호화하여 제공하고, 디바이스 처리기에서 처리되어 저장부의 보안디스크로부터 읽혀진 암호화된 데이터를 복호화 하여 보안디스크 서브시스템으로 제공한다.

◉ 보안디스크 생성 어플리케이션

보안 디스크 생성 어플리케이션은 보안 디스크 구성, 디스플레이 처리 및 입력 처리를 포함한다. 디스플레이 처리는 보안디스크 생성 어플리케이션이 구동된 컴퓨터의 화면에 보안디스크를 구비하는 저장 장치를 생성하기 위한 시작 섹터, 용량(보안디스크 크기) 및 디스크 볼륨 등을 입력할 수 있는 보안 디스크 생성 수단 등을 포함하는 사용자 인터페이스 수단을 표시한다. 입력 처리는 사용자 인터페이스 수단에 대응하는 입력을 수신 받아 보안디스크 구성부로 출력한다. 보안디스크 구성부는 디스플레이 처리로 사용자 인터페이스 수단을 제공하고, 그에 따라 입력처리를 통해 입력되는 보안디스크 생성 정보를 입력받고 암호키, 파괴키, 섹터 오프셋, 섹터 시작정보, 디스크 크기 정보, 디스크 볼륨 정보 등을 포함하는 디지털 키를 생성한 후, 보안디스크 처리기를 호출하여 저장부의 시작 섹터로부터 일정 크기의 디지털키 영역에 디지털 키를 암호화하여 저장하고 디지털 키가 저장된 이후의 데이터를 암호화하여 저장하고 디지털 키가 저장된 이후의 데이터를 암호화하여 저장하는 보안 데이터 영역을 가지는 보안디스크를 생성한다.

3.2 VIPDISK 관리 방법 및 시스템 동작

VIPDISK시스템의 관리 방법에는 보안디스크 생성 어플리케이션의 실행에 의해 생성 및 활성화되는 보안디스크 생성 어플리케이션이 일반 디스크와 디지털 키가 저장되는 디지털 키 영역 및 디지털 키에 의해 암호화되는 보안 데이터 영역을 구비하는 보안디스크를 포함하는 저장장치를 찾고, 보안설정모드에서 보안디스크 영역을 숨기고, 사용자의 사용자 비밀번호에 의해 보안설정모드 해제 요청시 어플리케이션부에 보안디스크 서브시스템을 마운트 하여 보안디스크의 볼륨이 보이도록 하여 보안디스크에 데이터를 입출력할

수 있도록 설정하는 보안디스크 활성화 과정 및 보안 디스크 서브시스템이 활성화된 보안디스크에 데이터를 입출력하는 보안디스크 사용과정이 포함된다.

Fig.4.에서 보여준 것 같이 보안저장장치 생성과정을 보안디스크 생성 어플리케이션이 디스플레이 처리부를 통해 보안디스크 설정 수단을 제공하고, 보안디스크 설정수단을 통해 보안디스크로 설정할 시작 섹터를 포함하는 용량을 입력받아 보안디스크를 설정하는 보안디스크 영역설정 단계 및 보안디스크 생성 어플리케이션이 시작섹터로부터 일정 용량의 디지털 키를 구성하는 디지털키 구성단계를 포함한다. 보안저장장치 생성과정은 디지털 키를 구비하는 열쇠 어플리케이션을 생성하는 열쇠 어플리케이션 생성단계를 포함한다. 해당 디지털 키는 디지털 영역 내에 둘 이상으로 구성되되 복수의 각 디지털 키의 시작 섹터 정보는 랜덤하게 구성된다. 보안디스크가 생성후, 해당 장치의 활성화 과정은 Fig.5.에 보여준 것과 같다.

즉 열쇠 어플리케이션이 실행 시 구동된 열쇠 어플리케이션이 커널 계층에 보안디스크 처리를 구성하는 보안디스크 처리기 구성단계, 열쇠 어플리케이션이 사용자 인터페이스 수단을 표시하는 사용자 인터페이스 표시 단계, 사용자 인터페이스 수단을 통한 보안디스

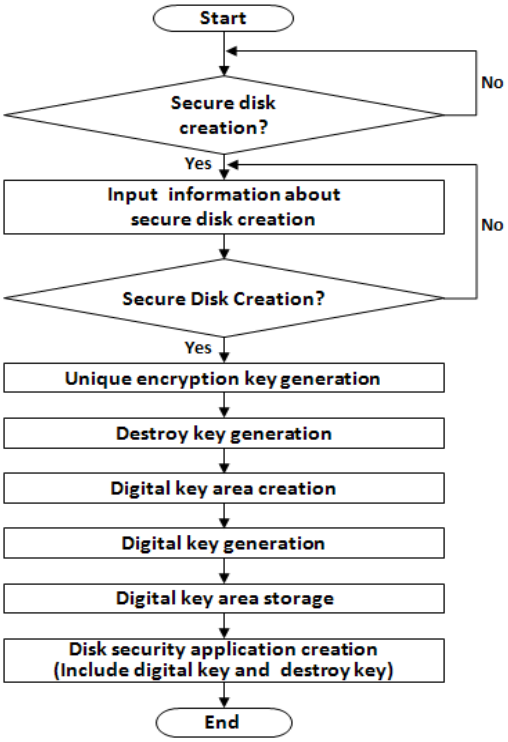

Fig. 4. Creation process of VIPDISK

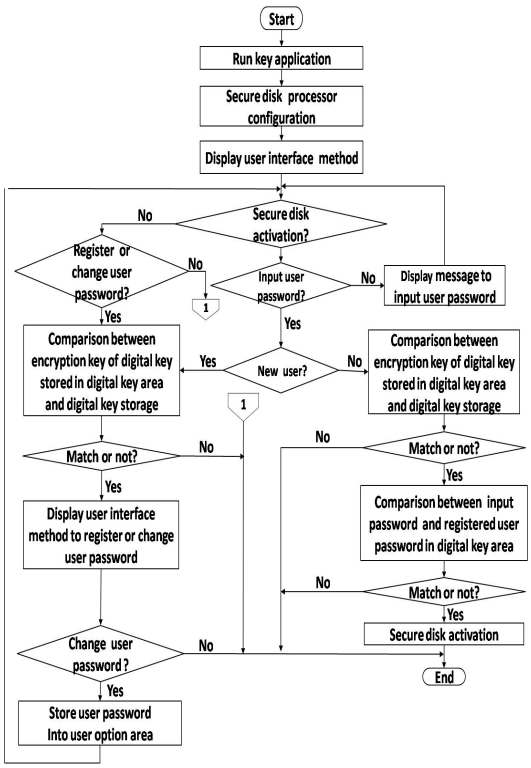

Fig. 5. Activation process of VIPDISK

크 활성화 요청이 발생되는지를 검사하는 보안디스크 활성화 요청 검사 단계, 활성화 요청이 발생되면 사용자 인터페이스 수단을 통해 입력되는 사용자 비밀번호가 입력되었는지를 판단하는 사용자 비밀번호 입력여부 판단단계, 및 사용자 비밀번호, 입력여부 판단에서 입력된 것으로 판단되면, 입력된 사용자 번호와 미리 설정되어 있는 비밀번호와 비교하여 일치하면 보안디스크를 활성화시키는 단계가 포함된다.

보안 디스크 활성화과정은 사용자 비밀번호 입력여부 판단 단계에서 사용자 비밀번호가 입력된 것으로 판단되면 미리 등록된 비밀번호 존재여부에 따라 처음 사용자인지를 판단하는 처음 사용자 판단 단계, 처음 사용자이면 사용자 비밀번호 등록 수단을 포함한 사용자 인터페이스 수단을 표시하는 사용자 비밀번호 등록 사용자 인터페이스 수단 표시단계, 사용자 인터페이스 수단을 통해 사용자 비밀번호 등록 단계를 포함한다. 보안디스크의 사용 중 보안디스크 비활성화 이벤트 발생시 FIg.6.과 같이 열쇠 어플리케이션이 보안 디스크 처리기를 삭제하고 운영시스템에 열쇠 어플리케이션의 구동 종료를 요청하여 보안 디스크 비활성화 시

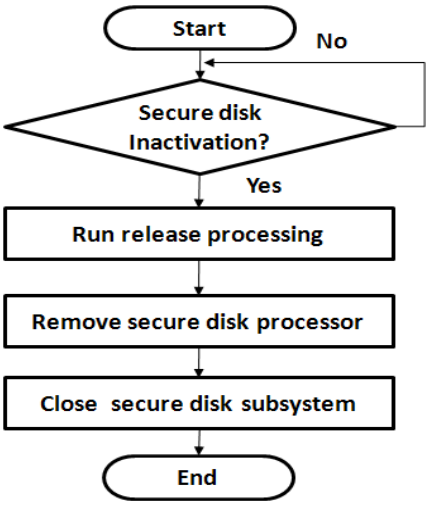

Fig. 6. Inactivation process of VIPDISK

킨다. 즉 보안 디스크 비활성화과정은 보안 디스크의 사용 중 열쇠 어플리케이션 구동 종료 이벤트의 발생 시 열쇠 어플리케이션이 구동 해제 처리기를 구동하여 등록 된 구성요소를 삭제하여 보안디스크 처리기를 제거단계 및 열쇠 어플리케이션이 운영시스템에 자신의 종료를 요청하여 구동을 종료하는 열쇠어플리케이션 구동종료 단계가 있다.

열쇠 어플리케이션이 열쇠 어플리케이션 활성화에 의해 표시된 사용자 인터페이스 수단을 통해 파괴 비밀번호의 입력 시 디지털 키의 파괴 비밀번호와 비교하여 일치하면 보안디스크의 디지털키 영역에서 디지털 키를 영구 삭제하여 보안디스크의 보안 데이터 영역에 저장된 데이터를 사용할 수 없도록 파괴하는 과정은 Fig.7.에 보여준 것과 같다.

보안디스크 파괴 과정후, 열쇠 어플리케이션이 디지털 키 보관소에 저장된 디지털 키의 시작섹터 정보 및 디지털 키 영역의 정보에 의해 파괴된 보안디스크의 디지털 키 영역에 디지털 키를 저장하여, 보안 디스크를 다시 활성화 시키는 파괴 보안디스크 복원 과정을 포함한다. 보안 디스크가 생성된 후, 보안 디스크를 구비하는 저장 장치가 연결되어 있는 컴퓨터에서 열쇠 어플리케이션은 커널계층에 보안 디스크 처리기를 생성한다. 열쇠 어플리케이션부는 보안 디스크 처리기를 생성 후, 화면상에 사용자 인터페이스 수단을 표시한 후, 사용자 비밀번호를 설정하고, 이후 설정된 비밀번호와 동일한 비밀번호를 입력 시 보안디스크 포함한 저장 장치를 검출하고, 보안디스크 처리부를 어플리케이션에 마운트 하여 검출된 보안디스크를 드라

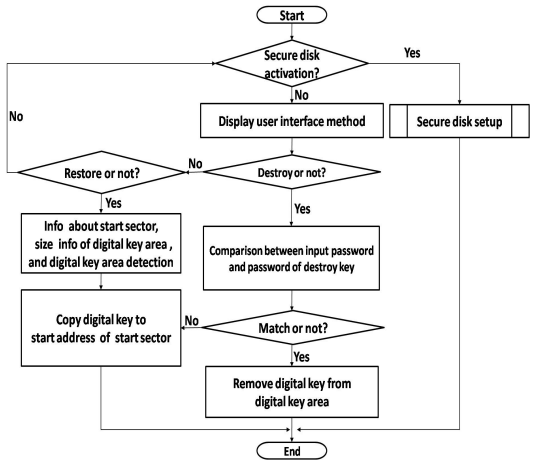

Fig. 7. Destruction and restoration process of VIPDISK

이브로 활성화시킨다. 이때 어플리케이션부에 마운트하여 검출된 보안디스크를 드라이브로 활성화시킨다. 이때 어플리케이션에 보안디스크가 가상의 볼륨으로 마운트 된다. 보안 디스크 활성화 후 어플리케이션은 보안 디스크를 일반 드라이브처럼 표시하고, 사용자의 요청에 따라 보안 디스크에 데이터를 저장하거나 읽어들여 보안디스크를 사용한다. 보안 디스크 사용 중에 보안 디스크 비활성화 이벤트의 발생 시 열쇠 어플리케이션은 커널 계층에 설치된 보안디스크 처리 및 보안디스크 서브시스템을 비활성화 또는 삭제하여 보안 디스크를 비활성화 시킨 후 자신도 종료한다.

IV. VIPDISK 기술 구현 및 성능검증

본 장에서는 VIPDISK기술에 대한 유효성 검증 및 실제적인 구현과 함께 성능 검증 실험을 진행한다. VIPDISK 기술은 Visual C++ 2010로 개발되고 우선 현재 적용된 운영체재는 Windows 7환경으로 구현되었다. 실제 사용된 열쇠 어플리케이션 윈도우 *.dll과 *.lib 형식으로 구성될 수도 있다. 제안 기술은 이미 국내 금융기관 공인인증서 KICASAFE로 적용하여 상용화된 새로운 개념의 원천기술로서 자체 성능 분석 및 검토를 위주로 진행한다.

4.1 VIPDISK 기술 구현

VIPDISK 기술은 사용목적 및 요구되는 보안특성에 따라 크게 Fake style과 Normal style로 구현

가능하다. 물론 하나의 디스크 상에 Fake style과 Normal style의 조합 및 여러 개의 VIPDISK 영역을 생성도 가능하다.

◉ Fake style:

VIPDISK의 Fake style을 사용하면 열쇠 프로그램만 다른 곳에 잘 보관하면 그 컴퓨터 전문가를 포함한 누구도 디스크 보안 영역이 존재한다는 것을 알 수 없다. Fake style 은 아래와 같이 구현된다.

- 1TB 크기의 임의의 외장 하드 디스크내에 830GB 크기의 VIPDISK 영역을 갖는 Fake style의 VIPDISK를 만든다. 디스크 관리자에서 확인해보면 일반 외장 하드와 특별한 차이점을 느낄 수 없다. (Fig.8.)
- 윈도우 탐색기에서 사용량 정보를 확인해도 일반적인 폴더나 파일, VIPDISK의 열쇠프로그램을 제외하곤, 830GB이상의 특별한 파일이 없다.(Fig.9.)
- VIPDISK의 열쇠 프로그램을 이용하여 비밀번호를 정상적으로 입력하고 VIPDISK를 열면 다음과 같이 830GB의 VIPDISK영역이 별도의 드라이브로 설정되어 사용할 수 있다.(Fig.10.)

Fig.10.에서 보면 931GB+830GB=1.7TB의 공간이 있는 것처럼 보이지만, 실제로는 VIPDISK기술에 의해 임의로 지정된 위치로부터 이후 830GB의 공간을 VIPDISK영역으로 사용할 수 있도록 해주는 구조인데 VIPDISK영역이 열린 후 저장하는 모든 데

Fig. 8. VIPDISK(Fake) invisible status in disk management without digital key activation

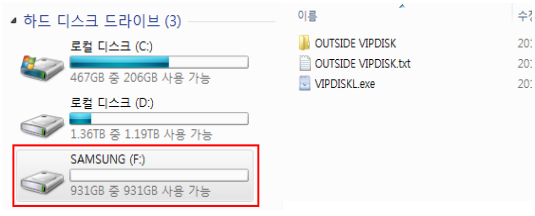

Fig. 9. VIPDISK(Fake) invisible status in windows explorer without digital key activation

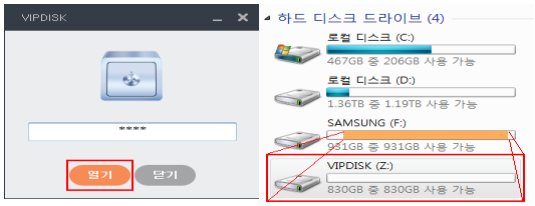

Fig. 10. A digital key application (left) & VIPDISK(Fake) visible status in windows explorer with digital key activation (right)

이터는 실시간으로 암호화되어 저장된다. Fake style은 자신의 디스크에 보안영역이 존재하는 것조차 알리고 싶지 않는 높은 보안특성을 가진다. 하지만 Fake style를 사용 시 주의할 점은 일반영역과 디스크의 공간을 일정부분을 공유하므로 VIPDISK영역이 시작되는 지점을 초과하도록 일반 영역에 많은 데이터를 저장하거나, 디스크를 Full format하는 경우에는 VIPDISK 영역이 소멸되는 단점이 있지만 VIPDISK 사용자는 할당된 보안 영역에 대한 정보를 알기 때문에 사전에 일반 영역의 오버플로우를 방지할 수 있다. 반면에 침입자 혹은 제 3자가 사용시 발생하면 오히려 보안 영역은 파괴될지라도 저장 데이터 유출을 오히려 방지할수 있게 된다. 다른 사용자 만약 Fake 영역의 존재를 발견 할지라도 열쇠프로그램 즉 디지털 키가 없이는 결코 보안 영역의 데이터를 액세스 할 수 없다.

◉ Normal style:

Normal style은 디스크를 일반 영역과 VIPDISK 영역으로 분할하여(필요시 복수의 VIPDISK 영역설정도 가능) 보다 안전하게 디스크를 사용할 수 있도록 제공해준다. Normal style 형태는 아래와 같이 구현된다.

- 1TB 크기의 외장하드 디스크를 400GB크기의 일반영역과 530GB의 VIPDISK 영역으로 분할하되 VIPDISK영역은 특성을 변경하여 포맷을 할 수 없도록 설정한다.(Fig.11.)

윈도우 탐색기에서는 기본적으로 400GB의 일반영역만 표시되며 일반 영역 내에는 자유롭게 일반적인 파일들을 저장할 수 있다. 물론 VIPDISK용 열쇠프로그램을 저장하면 편리할 수 있다.(Fig.12.)

Fig. 11. VIPDISK(Normal) invisible status without digital key activation in disk management

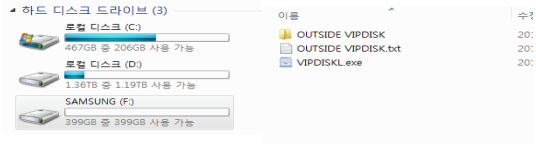

Fig. 12. VIPDISK(Normal) invible status without digital key activation in windows explorer

- VIPDISK의 열쇠 프로그램을 이용하여 비밀번호를 정상적으로 입력하고 VIPDISK을 열게 되면 400GB의 일반영역과는 별도로 530GB의 VIPDISK영역이 별도의 드라이브로 설정되어 사용할 수 있게 된다.(Fig.13.)

Normal style은 일반 영역과 VIPDISK영역이 파티션 레벨에서 완전히 분리되어 있기에 일반영역에 자유롭게 데이터를 저장하거나, Full Format등을 실행하더라도 VIPDISK 영역은 안전한 특성을 가진다. Fake style과 마찬가지로 VIPDISK 영역이 열린 후 저장하는 모든 데이터는 실시간으로 암호화 되어 저장된다.

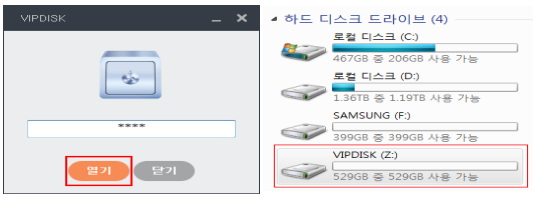

Fig. 13. A digital key application(left) & VIPDISK(Normal) visible status with digital key activation in windows explorer(right)

4.2 VIPDISK 성능 검증 실험

보안 디스크에 저장 데이터는 모두 암호화되었기에 사용자가 해당 저장 데이터를 액세스하게 되면 실시간으로 복호화를 해준다. 하지만 제안 기술은 데이터가 저장되는 보안디스크에서 암/복호화를 진행하기에 일반 디스크 제어보다 지연이 발생하게 된다. 실제로 VIPDISK에 저장된 임의의 비디오 동영상을 일반 디스크와의 성능 비교를 한 결과는 비디오가 플레이되는 과정에 영상과 음성 사이에서 모두 지연을 느낄 수 없었음을 관찰할 수 있었다. 왜냐 하면 저장 디스크의 I/O성능이 향상되고 컴퓨터 프로세싱 파워도 같이 높아지고 있기 때문에 제안 기법은 실시간 암/복호화가 가능하기 때문이다. 그 외도 실제로 대용량 100GB 크기의 임의의 데이터를 한꺼번에 보안 디스크에 복사해보면 일반 디스크에 똑같은 파일을 복사 할 때와 비교 실험 결과를 보면 5% ~ 7%의 I/O 지연이 관찰되는데 이는 암/복호화 과정에 피할 수 없이 발생되는 지연으로 관찰된다. 제안 기술은 암/복호화 알고리즘을 언제든지 필요에 따라 다른 종류의 암/복호화 기술로 대체가능하며 또한 제거도 가능하다. 추가 실험으로 VIPDISK 보안 디스크영역에 저장되어 있는 임의의 오피스 엑셀 파일(*.xls 혹은 *.xlsx)을 열어서 수정하고 저장한 다음 해당 보안 디스크가 활성화된 상태에서는 일반 디스크와 비교하였을 때 아무런 이상이 발생하지 않음을 확인할 수 있었다. 최근 보안 저장 디스크에 가장 많이 적용되는 기법들은 가상 이미지 디스크를 사용하는 기법과 보안 파티션을 이용하는 기법들이다. 이런 기존 기법들과 성능 비교분석을 위해 아래와 같은 실험을 진행한다.

4.2.1 이미지 파일형 가상 디스크[13]과의 성능비교

만약 가상 디스크 이미지 파일로 구성된 경우라고 가정하면 해당 영역을 정상 포맷하게 되면 모든 저장 데이터들은 사라지게 된다. 본 실험에서 임의의 D 드라이브를 VIPDISK 보안 디스크영역으로 지정한 다음 정상적인 포맷을 하게 되면 해당 D드라이브는 삭제되고 모든 저장 데이터도 삭제된 것처럼 보이게 된다. 하지만 포맷 완료후 다시 열쇠 어플리케이션을 통해 VIPDISK 보안 영역을 활성화시키면 해당 지역에 저장된 데이터들은 그대로 보존되고 저장된 파일을 다시 실행시켜도 정상임을 확인되었다.

4.2.2 보안 파티션 설정 기법과의 성능비교

기존의 보안 파티션을 설정한 경우도 위에 언급된 이미지 파일형태와 마찬가지로 해당 파티션을 지우면 저장된 모든 정보 데이터는 손실되어 사용할수 없다. 본 실험에서는 임의의 영역을 할당하여 VIPDISK 보안 디스크 영역으로 설정한 다음 해당 파티션을 지운다. 해당 파티션을 지우고 윈도우 탐색기를 열어보면

일단 파티션 드라이브가 사라져 저장된 데이터가 지워진 것처럼 보인다. 이 상태에서 열쇠 어플리케이션을 활성화 시키면 저장된 데이터를 열어보면 저장된 데이터에는 아무런 이상이 없으면 다시 보안 영역 드라이브가 활성화되고 정상 작동됨을 확인하였다. 위에 2가지 실험을 통하여 VIPDISK는 보안 파티션이나 이미지 형태의 가상 파일형태의 디스크와는 아무런 연관성이 없음을 보여주며 오히려 보안파티션이나 이미지 파일 기반의 기존 기법들의 약점을 극복하며 보다 강인한 보안성을 보여준다. 또한 OS도 모르게 보안 디스크를 제어하기에 보안성을 높이는 효과도 있었다.

4.2.3 보안디스크의 안정성 테스트 검증

제안 기술은 OS 모르게 디스크를 제어하는 기술을 보여주고 있지만 이런 기술이 만약 실행이 불안정하면 블루 스크린이 생기고 시스템 충돌이 발생하게 된다. 제안 기술의 안정 테스트를 위해 보안디스크가 활성화된 상태에서 보안 디스크 영역에 새 파티션을 만들어 본다. 정상적인 OS상태에서는 한 개의 파티션을 만든 다음 포맷을 실행한 다음 다시 열쇠 프로그램으로 보안디스크를 활성화 시키면 보안디스크에는 아무런 이상이 없고 저장된 파일을 열어봐도 별다른 이상이 없이 정상적으로 작동됨을 확인할 수 있었다.

결론적으로 Table 1.(Appendix에 표시됨)에서 보여준 것 같이 VIPDISK 의 성능을 카타고리별로 정리하여 일반 저장디스크,기존의 보안 저장장치와 비교분석해보면 VIPDISK의 보안 성능의 우수성을 알 수 있다. 추가로 스페인 InLabFIB(talent & tech)[14]에 의뢰하여 세계 각국의 수사기관 및 정보기관에서 가장 많이 활용하는 디지털 포렌직 제품 가이던스 소프트웨어의 인케이스로 VIPDISK를 검사해도 흔적을 찾을 수 없다고 테스트 결과 리포트를 받았다.

V. 결 론

본 논문에서는 보안 디스크가 비활성화상태에서는 운영시스템의 어플리케이션을 포함한 어떤 것에 의해서도 해당 보안 디스크의 존재 여부를 알 수 없으며 운영시스템에 무관하게 모든 디스크를 직접 제어하여 디스크의 물리적인 보안을 제공할 수 있는 VIPDISK 기술을 제안한다. VIPDISK 기술은 사용자가 설정한 비밀번호와 고유한 디지털 키를 가지는 고유의 열쇠 어플리케이션을 통해 저장장치의 임의의 용량을 가지고 디지털 키로 암호화된 보안디스크를 활성화 및 비활성화를 시킬 수 있으므로 강력한 보안성을 제공할 수 있는 효과를 갖는다.

특히 디지털 키 방식을 이용하여 보안디스크를 검출함으로써 기존 기술과 달리 매핑 테이블을 운영하지 않으므로 보안 디스크의 보안성을 높이는 효과를 갖는다. 그 외에도 미리 설정된 고유의 파괴키를 제공함으로써 사용자로부터 파괴키를 입력 시 디지털 키만 파괴시켜 디지털 키로 암호화된 보안 디스크 데이터에 접근 및 사용할 수 없도록 하여 데이터 유출을 방지할 수 있는 장점들이 있다. 그리고 파괴된 디지털 키를 포함하는 어플리케이션만 구비하고 있으면 디지털 키를 복사하는 것만으로 보안디스크에 저장된 데이터를 다시 활용할 수 있게 한다. 추가로 타이머를 구동하여 일정 시간동안 컴퓨터를 사용하지 않거나 대기화면 전환 이벤트가 발생되면 자동적으로 보안디스크를 잠그도록 함으로써 중요한 데이터 손실과 유출을 방지하는 보안성을 더욱 향상시키는 효과를 갖는다.

References

[1] Deyan Chen and Hong Zhao, "Data security and privacy protection issues in clouding computing," Proceedings of 2012 International Conference on Computer Science and Electronics Engineering, pp. 647-651, Mar. 2012.

[2] Youngmin Yeo, Chanwoo lee, and Jongsub Moon, "Proposal of security requirements for the cloud storage virtualization system," Journal of The Korea Institute of information Security & Cryptology, 23(6), pp. 1247-1257, Dec. 2013

[3] Jong-chang Ahn, Seung-won Lee, Ook Lee, and Sung phil Cho, "A study on influence of information security in selecting smart phone," Journal of The Korea Institute of information Security & Cryptology, 24(1), pp. 207-214, Feb. 2014

[4] DaeYeong Hong, WonSeok Ko, and Seongsoo Im, "Virtualization techniques for secure and reliable computing,"

Journal of The Korea Institute of information Scientists and Engineers, 26(10), pp. 50-57, Oct. 2014

〔5〕 Jungho Ju, Seungyoung Ma, and Jongsub Moon, "Proposal of security requirements for storage virtualization system against clouding computing security threats," Journal of Security Engineering, 11(6), pp. 469-478, Dec. 2014

〔6〕 Jong-shik Lee and Kyung ho Lee, "A study on security container to provent data leaks," Journal of The Korea Institute of Information Security & Cryptology, 24(6), pp. 1225-1241, Dec. 2014

〔7〕 Khelender Sasan, "Docker Containers," NEC Technologies India, Oct. 2014.

〔8〕 Kong Jae Hee, "Secure full-virtualization method," M.S. Thesis, SungKyunKwan University, Apr. 2013.

〔9〕 Hyewon Lee, Changwook Park, GuenGi Lee, KwonYoup Lee, and Sangjin Lee, "Analysis of present situation of secure USB from forensic view point," Proc. of The Korean Society of Broadcast Engineers, pp. 63-65, Feb. 2008

〔10〕 Ji-Hoon Jung, Suk-Hyun Kim, Min-Su Kim, and Bong-Nam Noh, "Analyze vulnerability of secure storage," Proc. of The Korean Institute of Information Scientists and Engineers, pp. 58-61, Nov. 2009

〔11〕 Byong Kuk Lee, "Memory system having secure storage device and method of managing secure area thereof," Patent (KR1020090067649), Jun. 2009

〔12〕 Suk-Jo Shin, Seon-Joo Kim, and In-June Jo, "Privacy data protection methods on smart phone using a virtual disk," Journal of The Korea Contents Association, 13(12), pp. 560-567, Dec. 2013

〔13〕 TaeSup Zang, "Understanding virtualized disk storage technology," Journal of The Korean Information Technology, 7(1), pp. 67-74, Dec. 2009

〔14〕 Manel Medina, "VIPDISK security report," esCERT at inLAB-UPC, Barcelona, Apr. 2015.

Appendix:

Table 1. Performance comparisons between general data storage device, previous secure storage devices and VIPDISK

Categories	General data storage device	Previous secure storage device	VIPDISK
Secure method	No	Password authentication	Triconnected encryption by using key application
Creation speed of secure storage	No	Varies depending on the secure method	Unrelated to the size of file or disk(less than one minute)
The usage of storage device	Easy	Some functions are difficult to use	Easy to use as windows explorer
Write or read speed	Fast	Depending on encryption and decryption methods	Use Direct I/O method as general storage device
Existence of data	Varifiable	Varifiable	Self-recognition of storage is impossible, can not varify existence of data
Data leakage	Possible for anyone	Possibility of hacking by expert hacker	Can not recognize existence of data, excluded from the hacking
Data status after format (Fast format)	Unusable	Unusable	Usable
Data status after remove partition	Unusable	Unusable	Usable(unrelated to OS)

〈저 자 소 개〉

전 선 국 (Shan Guo Quan) 정회원
1998년 7월: 중국 연변대학 과학기술학원 전자전산학과 공학사
2002년 8월: 강원대학교 제어계측학과 공학석사
2009년 8월: 연세대학교 전기전자공학부 공학박사
2009년 9월~2010년 2월: 연세대학교 BK21 TMS사업부 박사후연구원
2010년 3월~2012년 3월: 남서울대학교 전자공학과 교수
2012년 3월~현재: 중국 연변대학 과학기술학원 통신학과 교수
〈관심분야〉 무선 멀티미디어 통신, 정보 보안, IoT

권 용 구 (Yong-Gu Kwon) 정회원
1998년 7월~1997년 7월: 삼성전자 소프트웨어개발 프로그래머 직원
1998년 7월: 삼성경영기술대학 정보통신학과 졸업 및 강사 역임
2003년: (주) 아이오셀 연구소장 역임
(주) 비젯 부사장 역임
2008년~2009년: Intelligent Wave Korea Inc(IWKI) 수석 개발책임자
2009년~2013년: 지란지교소프트 연구원 및 컨설턴트 역임
2013년~현: 필립소프트웨어 대표
〈관심분야〉 정보보호, 보안 솔루션 연구개발