KOSDI
ISSN : 1976-2208 (Print)
ISSN : 2671-5287 (On-line)
www.sodi.or.kr

Journal of the Society of Disaster Information
Vol. 17, No. 4, pp. 897-903, December 2021
https://doi.org/10.15683/kosdi.2021.12.31.897

Original Article

불특정 위협으로부터 데이터를 보호하기 위한 보안 저장 영역의 생성 및 접근 제어에 관한 연구

A Study on Creation of Secure Storage Area and Access Control to Protect Data from Unspecified Threats

김승용[1] · 황인철[2]* · 김동식[3]
Seungyong Kim[1], Incheol Hwang[2]*, Dongsik Kim[3]

[1]Professor, Department of Management Information System, Korea National University of Transportation, Chungbuk, Republic of Korea
[2]Director, Secuware Inc., Cheongju, Republic of Korea
[3]Director, KCC Corporation, Seoul, Republic of Korea

*Corresponding author: Incheol Hwang, ichwang@secuware.co.kr

ABSTRACT

Purpose: Recently, ransomware damage that encrypts victim's data through hacking and demands money in exchange for releasing it is increasing domestically and internationally. Accordingly, research and development on various response technologies and solutions are in progress. **Method:** A secure storage area and a general storage area were created in the same virtual environment, and the sample data was saved by registering the access process. In order to check whether the stored sample data is infringed, the ransomware sample was executed and the hash function of the sample data was checked to see if it was infringed. The access control performance checked whether the sample data was accessed through the same name and storage location as the registered access process. **Result:** As a result of the experiment, the sample data in the secure storage area maintained data integrity from ransomware and unauthorized processes. **Conclusion:** Through this study, the creation of a secure storage area and the whitelist-based access control method are evaluated as suitable as a method to protect important data, and it is possible to provide a more secure computing environment through future technology scalability and convergence with existing solutions.

Keywords: Data Protection, Ransomware, Storage, Secure Area, Access Control

요 약

연구목적: 최근 국내외에서 해킹으로 피해자의 데이터를 암호화하고 이를 풀어주는 대가로 금전적 대가를 요구하는 랜섬웨어 피해가 증가하고 있다. 이에 다양한 방식의 대응기술과 솔루션에 대한 연구개발이 진행되고 있으며, 본 연구에서는 데이터를 저장하는 저장장치에 대한 보안 연구개발을 통해 근본적인 대응방안을 제시하고자 한다. **연구방법:** 동일한 가상환경에 보안 저장영역과 일반 저장영역을 생성하고 접근 프로세스를 등록하여 샘플 데이터를 저장하였다. 저장된 샘플 데이터의 침해 여부를 확인하기 위해 랜섬웨어 샘플을 실행하여 침해 여부를 해당 샘플 데이터의 Hash 함수를 확인하였다. 접근제어 성능은 등록된 접근 프로세스와 동일한 이름과 저장위치를 통해 샘플 데이터의 접근 여부를 확인하였다. **연구결과:** 실험한 결과 보안 저장 영역의 샘플 데이터는 랜섬웨어 및 비인가된 프로세스로부터 데이터의 무결성을 유지하였다. **결론:** 본 연구를 통해 보안 저장영역의 생성과 화이트리스트 기반의 접근 제어 방법이 중요한 데이터를 보호하는 방안으로 적합한 것으로 평가되며, 향후 기술의 확장성과 기존 솔루션과의 융합을 통해 보다 안전한 컴퓨팅 환경을 제공할 수 있을 것으로 기대된다.

핵심용어: 데이터보호, 랜섬웨어, 저장장치, 보안영역, 접근제어

Received | 3 December, 2021
Revised | 23 December, 2021
Accepted | 23 December, 2021

Introduction

최근 국내·외에서 해킹으로 피해자의 데이터를 암호화하고, 이를 풀어주는 대가로 가상화폐를 이용한 금전적 이득을 취하려고 하는 랜섬웨어(Ransomware) 피해가 증가하고 있다. 미국에서 랜섬웨어 공격은 송유관·육가공업체 등 기반시설과 국민 생활에 밀접한 분야가 목표가 되어 국가적 혼란을 일으키기도 했다. 우리나라도 피해가 증가 중이며, 보안 투자 여력이 부족한 중소기업을 중심으로 다양한 분야에서 피해가 발생하고 있다.

최근의 랜섬웨어 공격은 프로그래머가 랜섬웨어를 제작하여 범죄조직에 공급하고 수익을 공유하는 서비스형 랜섬웨어(Ransomware as a Service)가 증가함에 따라 범죄형태가 분업화되고 조직화되고 있다. 이러한 사이버공격에 체계적으로 대응하지 못하면 향후 사회적·경제적으로 큰 피해가 예상된다.

사이버공격의 대부분이 상대적으로 해킹 및 악성코드의 유포가 쉬운 엔드포인트 PC를 공격하여 권한 상승을 통해 서버를 해킹하는 방식으로 진화하고 있다(Kim et al., 2014). 이러한 공격으로 인해 중요 데이터의 암호화 및 유출 피해가 발생하고 있으며, 기업 등 피해기관은 중요 데이터의 복구 및 정보유출에 대한 대응으로 상당한 시간과 비용을 지불하고 있는 실정이다.

다양한 위협에 의한 데이터 침해를 예방하기 위해 개발된 기존의 보안 솔루션들은 사용자 컴퓨터에 설치되는 운영체제에 의해 제어되는 기술을 사용하고 있다. 즉, 모든 데이터가 전통적인 파일 저장방식의 인터페이스를 사용하고 있어 악성코드 또한 해당 데이터를 공격할 수 있는 기회를 제공한다. 이러한 저장방식의 특징으로 보안 기능을 구현하는데 어려움이 있으며, 운영체제의 취약점으로 인해 보안 기능이 작동하지 않을 수 있는 문제도 있다(Kim et al., 2007).

본 연구에서는 사이버 공격의 대상이 되는 데이터의 안전한 보관을 위한 보안 저장영역의 생성과 보안 저장영역의 접근제어 방법에 대한 연구를 통해 다양한 침해요소로부터 데이터 보호 성능을 실험하였다.

Data Storage Methods

거의 모든 개인용 컴퓨터는 Fig. 1과 같이 메타 데이터 영역과 사용자 데이터 영역의 구조를 유지하고 있다. 즉, 물리적인 저장장치에 데이터 저장공간을 구성하기 위해 필요한 파티션 테이블 정보와 파일 테이블 정보 등 메타 데이터를 저장하는 논리 파티션을 구성하고 있다. 논리 테이블 내의 메타 데이터는 암호화되어 저장되지 않으며, 이미 그 구조에 대한 정보가 공개되어 있어 손쉽게 역분석(Reverse Engineering)이 가능하다. 이러한 논리적 파티션의 시작 위치, 크기 등 메타 데이터는 표준으로서 일정한 오프셋이 지정되어 있다. 이러한 표준구조는 전문적인 데이터 복구 프로그램이나 디지털 포렌식 등 그 구조를

Fig. 1. Traditional data storage method

분석함으로써 중요 데이터를 유출할 수 있으며, 해킹 등 비인가자 또는 악성코드 등에 의해 저장공간 내 중요 데이터가 암호화 등 위변조되거나 유출될 수 있다.

즉, 운영체제에 의해 생성된 저장영역의 데이터는 파일 형태로 저장되기 때문에 기존의 데이터 보호 기술 또는 제품뿐만 아니라 악성코드에 의해서 데이터 손상이 가능하며, 보안 솔루션을 우회하는 등 인가되지 않은 사용자 또는 프로세스에 의해 데이터 접근이 가능하다. 이러한 위변조 가능성은 일반적인 데이터 업무환경 외에 디지털 포렌식 분야에서도 디지털 증거물의 무결성을 보장하기 어렵다(Kim et al., 2017).

저장장치의 중요 데이터를 보호하기 위해 해당 파일을 암호화하거나 디렉터리(폴더)를 암호화하는 방법이 제시되었지만 보안 취약점이 알려지면서 효용성이 떨어졌다. 대안으로 가상볼륨을 생성하여 중요 데이터를 일반 영역과 분리하여 보호하는 기술들이 제시되었다(Hong et al., 2014; Ju et al., 2014). 일례로 윈도우 운영체제에서는 하이퍼바이저(Hypervisor) 기술을 기반으로 가상화 컨테이너를 구성한다(Lee et al., 2014). 그 외에 대부분의 가상화 기술들이 전통적인 파일시스템 상에 컨테이너 형태로 존재하기 때문에 해당 컨테이너 자체의 손상 또는 가상화 컨테이너의 분석을 통해 중요 데이터의 분석이 가능하다.

상기 문제점을 근본적으로 해결하기 위해 선행연구에서 Fig. 2와 같은 데이터보호 기술 구조의 보안영역을 생성하는 방법에 대해 실험하였다. 일반 저장부는 기존의 전통적인 방식으로 생성되어 운영체제가 인식 가능한 형태의 파티션 정보를 가지고 있다. 반면 보안 저장부는 운영체제가 해당 영역의 데이터를 입출력할 수 없는 구조의 암호화된 가상드라이브 형태를 가지고 있다. 실험을 통해 운영체제에 독립적인 저장영역을 생성하였고, 실험 데이터를 해당 저장영역에 실시간 암복호화하는 것을 확인하였다(Kim et al., 2021).

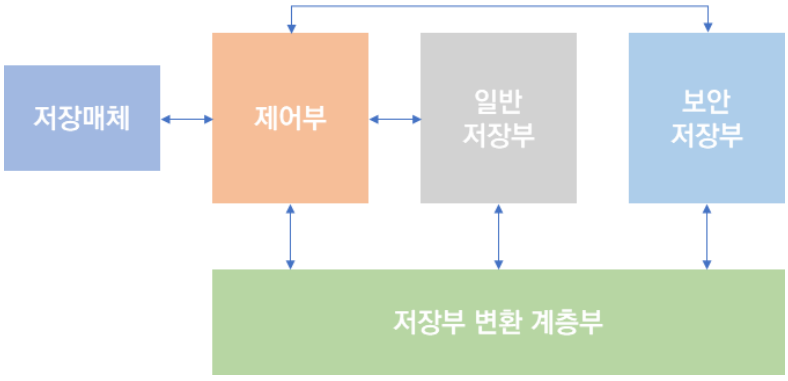

Fig. 2. Configuration diagram of data protection technology

본 연구에서는 Fig. 3에서 보는 것과 같이 기존의 보안 저장영역 생성의 한계를 극복하여 다양한 저장장치에 다양한 형태의 보안 저장영역을 생성할 수 있도록 하였다.

컴퓨터 선택을 통해 로컬 컴퓨터뿐만 아니라 서버에 등록된 원격지 컴퓨터의 저장장치에도 보안 저장영역을 생성할 수 있도록 구현하였다. 이는 향후 기업 등 대단위 사용자 환경에서 보안 저장영역의 생성 등 원격지 관리가 가능할 것이다.

보안 저장영역을 생성하기 위한 과정으로 해당 컴퓨터에 연결되어있는 모든 저장장치를 검색한다. 검색된 각 저장장치의 파티션 및 파일시스템 정보를 확인하여 보안 저장영역의 생성이 가능한지 판단하여 사용자에게 제공한다. 보안 저장영역의

생성이 가능한 파티션은 NTFS 기반으로 한정하였다. 선택한 파티션에 생성하고자 하는 용량을 입력하면 NTFS의 볼륨 축소 기능을 활용하여 입력한 크기만큼 기존 파티션을 축소하고 보안 저장영역을 위한 새로운 파티션을 생성한다. 기존 파일 시스템이 MBR 방식이면 OEM 파티션으로 생성하고, GPT 방식이면 Reserved 파티션으로 생성하여 윈도우 파티션 관리자에서 보이지 않도록 한다. 기존 파티션을 축소한 후 보안 저장영역의 생성에 필요한 정보를 신규 파티션에 암호화하여 기록한다. 해당 정보는 저장장치의 시리얼번호, 보안 저장영역의 크기 등 보안 저장영역을 식별할 수 있는 고유한 값들로 구성된다.

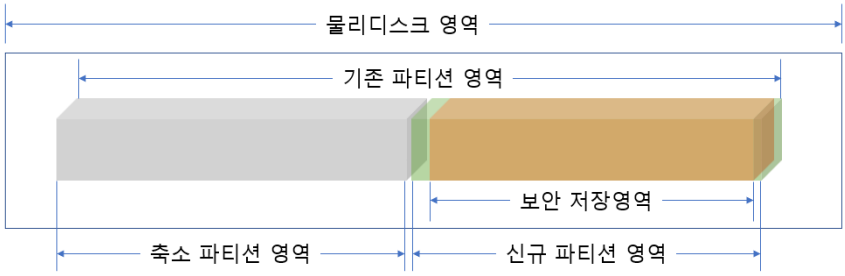

Fig. 3. Making secure area

본 연구에서는 상기와 같이 NTFS의 볼륨축소 영역뿐만 아니라 파티션 전체를 보안 저장영역으로 생성할 수 있도록 별도의 기능을 구현하였다. 이를 통해 저장공간의 낭비 없이 보안 저장영역을 최대한 확보할 수 있다.

Process Access Control Method

보안 저장영역의 생성에도 불구하고 해당 보안영역에 대한 데이터 입출력을 위해서는 운영체제에 마운트하는 과정을 거치게 된다. 즉, 일반 영역과 같은 저장영역에 대한 드라이브 레터를 부여받게 되며, 이는 사용자뿐만 아니라 악성코드 등 침해요소도 동일하게 데이터 접근이 가능하다는 한계를 가지고 있다. 물론 보안 저장영역의 마운트가 해제되면 보안 저장영역 또한 보이지 않게 되어 공격의 대상이 되는 데이터가 없게 된다.

그럼에도 불구하고 비인가된 데이터 접근을 방지하기 위한 여러 연구들이 진행되었고 관련 솔루션이 출시되었다. 대표적인 데이터 접근 제어 방식으로는 데이터에 접근할 수 있도록 허용된 프로세스를 등록하여 모니터링과 제어를 하는 것이다. 허용된 프로세스의 등록은 프로세스의 이름을 기반으로 등록하는 것과 해당 프로세스의 저장위치를 포함하여 등록하는 방식이 있다. 이러한 방식은 프로세스의 이름 또는 저장위치 등을 위변조함으로써 불법적인 데이터 접근이 가능할 수 있다.

따라서 본 연구에서는 생성된 보안 저장영역에 접근을 허용할 프로세스를 안전하게 등록하고 유지하는 방안이 필요하였다. 실험에 적용한 방식은 운영체제에서 실행되고 있는 모든 프로세스와 실행 가능한 프로세스를 조사하여 사용자에게 제공하는 것이다. 이를 통해 사용자는 프로세스별 차단 또는 읽기전용 또는 읽기·쓰기 허용을 선택할 수 있다. 사용자가 등록한 신뢰 프로세스를 기반으로 보안 저장영역의 접근을 제어한다.

Fig. 4에서 프로세스 이름은 해당 프로세스의 실제 파일명을 표출한다. 프로세스 해시는 프로세스 이름을 임의로 변경하여 접근제어 정책을 우회할 수 없도록 각 프로그램의 지문정보를 취득하여 접근제어에 사용한다. 프로세스 구분은 각 프로세스의 현재 상태를 표시하는 것으로 '실행중'은 현재 실행 중인 프로세스를 의미하며, '프로그램'은 시스템에 설치된 프로그램임

을 의미한다. 프로세스 권한에서는 상기한 것처럼 1개 이상의 프로그램을 읽기' 또는 '읽기/쓰기'로 지정해야 프로그램 접근 제어가 활성화되며, 아무런 프로그램도 지정하지 않은 경우에는 모든 프로그램의 접근이 허용되도록 정책을 설계하였다.

Fig. 4. Process access control

Experimental Design

본 연구에서는 선행연구의 보안 저장영역을 생성하는 방법에 대한 고도화를 통해 다양한 저장장치 및 파일 시스템에서 보안 저장영역을 생성할 수 있도록 하였다. 기존 연구에서 보안 저장영역을 생성하는 방법으로는 NTFS 파일 시스템에만 적용하였고 마이크로소프트사의 윈도우 기능인 볼륨 축소를 통해 축소된 영역에 보안 저장영역을 생성하였다. 본 연구에서는 기존 방식은 물론 NTFS 전체 영역을 보안 영역으로 설정하는 기능을 추가하여 보안 저장영역을 최대 크기로 생성할 수 있도록 하였다. 실험의 대조군으로는 전통적인 디스크 구조를 가지는 NTFS 방식의 일반 저장영역을 생성하였다.

보안 저장영역에 대한 접근제어 방법으로는 Fig. 5와 같이 화이트리스트 기반의 접근제어 방식을 적용하였다. 화이트리스트는 사용자가 신뢰 프로세스를 선택하면 해당 프로세스의 Hash 값을 취득하고 프로세스 저장 위치 및 디지털 서명을 취득하여 프로세스 위변조 등 우회하지 못하도록 하였다.

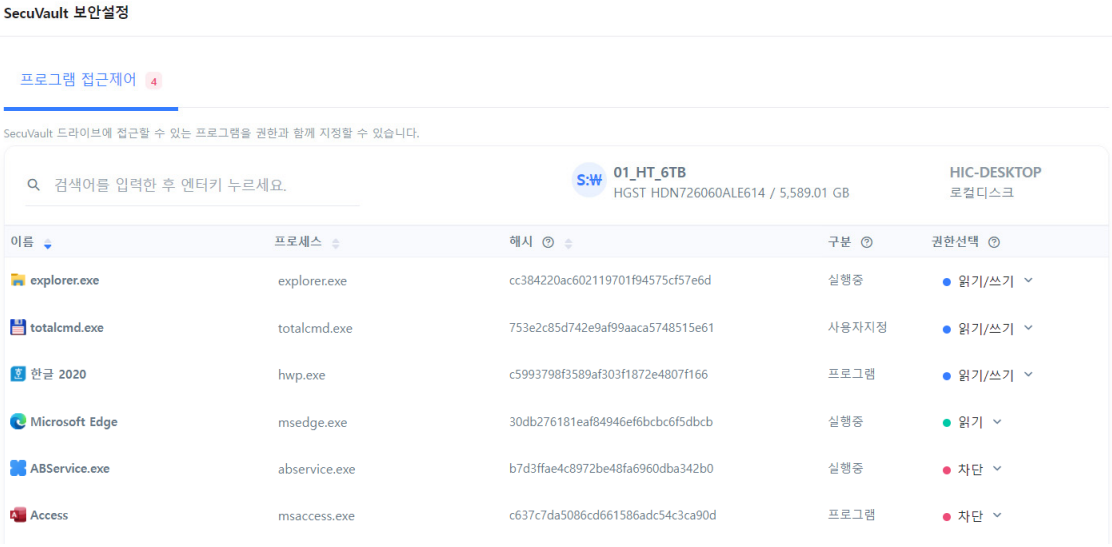

Fig. 5. Setting access control processes

실험을 위해 대표적으로 사용되는 파일을 생성하고 해당 파일의 Hash를 확보하였다. 실험 파일들은 보안 저장영역과 일반 저장영역에 동일하게 저장하였고, 해당 파일의 침해여부를 실험하기 위해 랜섬웨어 샘플을 시스템에 작동시켜 실험 파일들이 손상되는지 확인하였다. 또한, 프로세스 접근제어의 성능을 확인하기 위해 등록된 프로세스와 동일하게 파일명을 변경하고 해당 저장위치에 저장하여 실행하였다.

Results

생성한 보안 저장영역에 샘플 데이터를 저장하고 입출력 테스트를 한 결과 Table 1과 같이 실험 파일의 무결성이 유지되었다. 보안 저장영역은 실시간 암호화를 통해 저장되며, 보안 저장영역에서 해당 파일을 열면 자동으로 복호화되어 사용자는 암복호화를 별도로 수행하지 않고도 보안이 강화된 컴퓨팅 환경을 제공받을 수 있다.

접근 제어 프로세스를 우회하는 실험에서는 접근 제어 목록에 등록된 프로세스의 이름과 저장 위치를 위변조하였음에도 불구하고 해당 보안 저장영역에 접근하지 못했다. 저장장치를 다른 PC에 연결하여 실험하였음에도 비인가된 프로세스는 보안 저장영역에 접근하지 못했다. 이는 접근 제어 정보가 프로그램에 저장되는 것이 아니라 보안 저장장치의 메타영역에 저장되기 때문에 저장장치를 임의로 이동하여 접근 시도를 해도 기존 접근 제어 정책이 유지된다. 뿐만 아니라 보안 저장영역에 저장되는 데이터와 마찬가지로 메타 데이터도 암호화되어 저장하기 때문에 그 구조나 정책에 대한 분석이 불가능하도록 하였다.

Table 1. Comparison of hash of normal storage and secure storage after ransomware infection

	Contents	Hash(MD5)
Sample file	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7
Normal area1	PK ?_Q # Sample_Origin.txt? AE V?-jW_?pV?K Dk ?? *PK ?_Q # Sample_Origin.txt? AE PK J]	61b6206a609f3b2b12645cbcf268dec1
Secure area1	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7
Normal area2	PK ?_Q ' Sample_Origin.txt? AE oB^p?g?3?5?e*?u CXPK ?_Q ' Sample_Origin.txt? AE PK J a	150ee612606fcd2b25b33e86f00d4d5e
Secure area2	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7
Normal rea3	PK ?_Q + Sample_Origin.txt? AE ?`f9V(S@ J?g%/??PK ?_Q + Sample_Origin.txt? AE PK J e	f7af52e4a989c41f81f07f7b2168a23d
Secure area3	Sample_Origin	5b7dd3cb7ea25dce573a5cfb27fb86e7

Conclusion

본 연구에서는 보안 저장영역을 생성하고 접근 제어 방법을 적용함으로써 기존의 보안 솔루션을 무력화 또는 우회하여 침

투한 악성코드 등으로부터 중요 데이터를 보호할 수 있음을 확인하였다. 이러한 기반 기술을 확장하고 기존 보안 솔루션과 융복합하여 보안이 강화되고 사용자 편의성이 증대된 컴퓨팅 환경의 제공이 기대된다.

Acknowledgement

본 연구는 2021년 한국교통대학교의 지원을 받아 수행하였음.

References

[1] Hong, D.Y., Ko, W.S., Im, S.S. (2014). “Virtualization techniques for secure and reliable computing.” Journal of The Korea Institute of Information Scientists and Engineers, Vol. 26, No. 10, pp. 50-57.

[2] Ju, J.H., Ma, S.Y., Moon, J.S., (2014). “Proposal of security requirements for storage virtualization system against clouding computing security threats.” Journal of Security Engineering, Vol. 11, No. 6, pp. 469-478.

[3] Kim, C., Choi. D., Yi. J., Kim. J. (2014). “A study of program execution control based on Whitelist.” Proceedings of the Korea Institute of Information and Communication Science Conference, KIICE, Korea, pp. 346-349.

[4] Kim, J.G., Kim, T.E., Choi, J.W., Kim, W.G., Lee, J.S. (2007). “Vulnerability analysis and research on digital contents storage system.” Journal of Information and Security, Vol. 7, No. 4, pp. 36-41.

[5] Kim, S.Y., Kim, G.Y., Hwang, I.C., Kim, D.S. (2017). “e-forensic tool research for obtaining legal evidence ability of digital evidence by intelligence inspection.” 2017, Vol. 13, No. 2, pp. 267-275.

[6] Kim, S.Y., Hwang, I.C., Kim, D.S. (2021). “A study on next-generation data protection based on non file system for spreading smart factory.” Journal of the Society of Disaster Information, Vol. 17, No. 1, pp. 176-183.

[7] Lee, J.S., Lee, K.H. (2014). “A study on security container to prevent data leaks.” Journal of The Korea Institute of Information Security & Cryptology, Vol. 24, No. 6, pp. 1225-1241.