보안 외장 하드디스크 취약점 익스플로잇 프레임워크 설계

홍세준[O], 정원빈[*], 권수진[*], 이경률[*]
[O]목포대학교 정보보호학과,
[*]목포대학교 정보보호학과
e-mail: {s193828[O], goblebin[*], sujiniya[*]}@mokpo.ac.kr, carpedm@mnu.ac.kr[*]

Design of a Vulnerability Exploit Framework for Secure External Hard Disks

Sejun Hong[O], Wonbin Jeong[*], Sujin Kwon[*], Kyungroul Lee[*]
[O]Dept. of Information Security Engineering, Mokpo National University,
[*]Dept. of Information Security Engineering, Mokpo National University

● 요 약 ●

기존의 외장 하드디스크는 보안 기능의 부재로 인하여, 비인가자로부터 디스크가 탈취되는 경우에는 저장된 데이터가 유출되거나 훼손되는 문제점이 존재한다. 이러한 문제점을 보완하기 위하여, 보안 기능을 제공하는 보안 외장 하드디스크가 등장하였지만, 보안 기능 중 패스워드나 지문 인증과 같은 사용자 인증을 우회하는 취약점이 지속적으로 발견됨으로써, 비인가자가 장치 내부에 안전하게 저장된 데이터에 접근하는 보안위협이 발생하였다. 이러한 보안위협은 국가사이버안보센터에서 공개한 보안 요구사항을 만족하지 못하거나, 만족하더라도 설계나 구현 과정에서 내포된 취약점으로 인하여 발생한다. 본 논문은 이와 같이 보안 외장 하드디스크에서 발생하는 취약점을 점검하기 위한 목적으로 보안 외장 하드디스크 익스플로잇 프레임워크를 설계하였다. 취약점을 점검하기 위한 전체 프레임워크를 설계하였고, 프레임워크에서 제공하는 각 기능 및 유즈케이스 다이어그램을 설계하였으며, 설계된 프레임워크를 활용한다면, 현재 상용화되었거나 추후 개발될 보안 외장 하드디스크를 대상으로 안전성을 평가할 것으로 판단된다. 그뿐만 아니라, 안전성 평가 결과를 기반으로, 보안 외장 하드디스크에 내재된 취약점을 보완함으로써 안전성을 더욱 향상시키고, 수동으로 분석하여야만 하는 보안 외장 하드디스크의 취약점 점검을 자동화함으로써, 안전성을 평가하는 시간과 비용 또한 절감할 것으로 사료된다.

키워드: 외장 하드디스크(external hard disk), 데이터 보호(data protection), 익스플로잇 프레임워크(exploit framework)

I. 서론

이동형 저장장치는 자료를 손쉽게 옮기는 기능을 제공하는 휴대용 저장장치이며[1], 외장 하드디스크는 일반적으로 USB 저장장치보다 저장용량이 크기 때문에, 대용량의 데이터를 저장할 수 있는 특징이 있다[2]. 그러나, 만약 외장 하드디스크가 비인가자에 의하여 탈취되는 경우, 저장된 데이터가 훼손되거나 유출될 가능성이 높으며, 이러한 문제점을 보완하기 위하여 보안 기능을 제공하는 보안 외장 하드디스크가 등장하였다[3].

보안 외장 하드디스크에서 제공하는 보안 프로그램은 사용자 인증 기술인 패스워드, 지문, 홍채, 키패드, NFC(Near Field Communication)와 같은 다양한 인증 방식 중 하나를 적용함으로써, 사용자를 식별하고 비인가자로부터의 접근을 차단하여 보안 외장 하드디스크를 안전하게 보호한다[4].

그러나, 보안 외장 하드디스크와 같은 이동형 저장장치를 대상으로, 역공학을 이용하여 패스워드 인증 우회나 지문 인증 우회와 같은 소프트웨어나 하드웨어 취약점을 악용함으로써, 비인가자가 저장장치 내부에 안전하게 저장된 데이터에 접근하는 취약점이 공개되었으며[5], 이러한 취약점은 지속적으로 발견되어 공개되는 추세이다[6]. 이에 따라, 해당 취약점을 악용한다면, 저장장치 내부에 안전하게 저장된 데이터의 기밀성과 무결성을 제공하지 못하는 문제점이 발생하며, 이러한 취약점을 사전에 탐지하고 조치하기 위하여, 보안 외장 하드디스크에 내재된 취약점을 발견하는 방안이 요구된다. 또한, 취약점을 점검하기 위하여, 보안 프로그램 대상으로, 역공학 기법이나

코드 분석을 이용하여 수동으로 취약점을 점검하거나 분석한다면, 시간과 비용 측면에서 낭비되는 자원이 증가할 것으로 판단되며, 더욱 효과적으로 취약점을 탐지하고 조치하기 위한 방안이 요구된다.

이와 같이, 취약점을 탐지하고 조치하기 위하여, 기존에는 메타스플로잇, 네서스, 넷스파커와 같은 취약점 익스플로잇 프레임워크들이 공개되어 있지만, 이러한 프레임워크들은 주로 시스템, 웹 애플리케이션, 소프트웨어 개발 프로세스 등을 대상으로 취약점을 점검하고 공격하기 때문에, 보안 외장 하드디스크를 대상으로, 취약점을 점검하는 도구나 프레임워크는 부재한 실정이다. 이에 따라, 보안 외장 하드디스크에 특화된 익스플로잇 프레임워크가 요구된다.

따라서, 본 논문에서는 이러한 요구사항을 만족하기 위하여, 보안 외장 하드디스크를 대상으로, 취약점 익스플로잇 프레임워크를 제안하고 설계하였으며, 설계한 프레임워크를 활용한다면, 보안 외장 하드디스크에 내재된 취약점을 효과적으로 진단할 것으로 판단된다.

II. 배경지식 및 관련 연구

1. 보안 외장 하드디스크

보안 외장 하드디스크는 하드웨어 방식과 소프트웨어 방식을 통하여, 외부의 위협으로부터 데이터를 안전하게 보호한다. 하드웨어 방식은 암호화 칩을 사용하여 보안영역을 제공하며, 소프트웨어 방식은 별도의 암호화 칩을 사용하지는 않지만, 소프트웨어인 보안 프로그램을 통하여 보안 영역을 제공한다.

이와 같은 보안 외장 하드디스크의 보안 요구사항으로, 국가사이버안보센터에서 정의한 소프트웨어 기반 보안 USB 제품 보안 요구사항을 살펴보면, 기밀성 및 사용자 인증, 접근통제, 사용자 인증을 정의하였다. 기밀성은 비인가자로부터의 데이터의 노출을 방지하는 것이며, 사용자 인증은 정당한 사용자의 접근만 허용하는 것이다. 접근통제는 인가된 관리자가 설정한 접근통제 정책에 따라 보안 USB 메모리에 저장된 데이터에 대한 접근을 허용 및 차단하는 것이다[7, 8].

상기 보안 요구사항에 만족하기 위하여, 보안 외장 하드디스크에서 제공하는 핵심 기능으로는 데이터 암호화 및 사용자 인증이 있다. 데이터 암호화는 저장장치 내부에 저장되는 데이터를 암호화함으로써 비인가자가 저장된 정보에 무단으로 접근하는 것을 방지하는 기능이며, 사용자 인증은 하드웨어 관점에서의 키패드, 생체인식, RFID(Radio-Frequency IDentification) 방식과 소프트웨어 관점에서의 패스워드 방식과 같은 다양한 인증 방식으로 사용자를 식별함으로써 비인가자로부터의 접근을 보호하는 기능이다.

2. 보안 외장 하드디스크의 사용자 인증 과정

보안 외장 하드디스크에서 제공하는 사용자 인증 과정의 일례를 그림 1에 나타내었다.

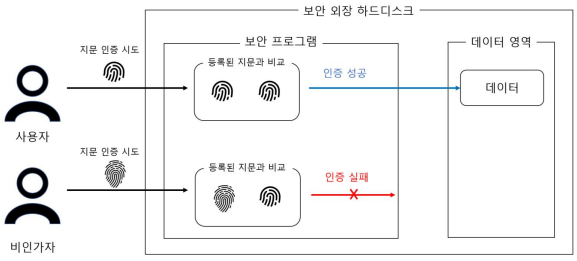

Fig. 1. 사용자 인증 과정 일례

그림에서 나타낸 것과 같이, 사용자가 보안 외장 하드디스크에 접근을 시도하면, 보안 프로그램이 실행되어, 해당 보안 외장 하드디스크에서 제공하는 인증 방식에 따라, 사용자로부터 입력받은 정보를 등록된 인증정보와 비교함으로써, 사용자를 인증한다. 정상적으로 사용자가 인증되는 경우에는 내부 데이터 영역으로의 접근을 허가하며, 인증되지 않은 경우에는 비인가자로 식별하여 접근을 차단한다.

3. 보안 외장 하드디스크의 패스워드 인증 취약점

기존 보안 외장 하드디스크에서 발견된 패스워드 인증 취약점을 살펴보면, 특정 상용 제품을 대상으로, 역공학 도구를 이용하여 보안 프로그램을 분석한 결과, 그림 2와 같이 사용자가 등록한 패스워드가 그대로 노출되는 취약점이 발견되었다[6].

```
76D10880   8BFF          MOV EDI,EDI
76D10882   55            PUSH EBP
76D10883   8BEC          MOV EBP,ESP
76D10885   5D            POP EBP
76D10886 - FF25 680CD776 JMP DWORD PTR DS:[<&KERNELBASE
```

```
004FD548  00F875C2  CALL to lstrcmpW from
004FD54C  00F1BA20  String1 = "qwerqwer"
004FD550  00F1A82C  String2 = "boss"
```

Fig. 2. 패스워드 비교 함수 코드 일례[6] (위: 취약점이 발생하는 코드 일례, 아래: 스택에 저장된 데이터 일례)

그림을 살펴보면, 문자열을 비교하는 함수인 lstrcmpW() 함수를 호출할 때, 입력한 패스워드(String 1)와 등록된 패스워드(String 2)가 그대로 노출된다. 이에 따라, 공격자는 등록된 패스워드인 String 2에 저장된 "boss"를 탈취할 수 있으며, 탈취한 패스워드를 입력하는 것만으로도 사용자 인증을 우회하여, 저장장치 내부에 안전하게 저장된 데이터의 탈취가 가능하다.

이와 같이, 사용자 인증의 우회나 복호키 노출과 같은 취약점은 다양한 보안 외장 하드디스크에서 발생할 수 있으며, 이러한 취약점으로부터 보안 외장 하드디스크의 안전성을 점검하기 위한 방안이 요구된다.

III. 보안 외장 하드디스크 취약점 익스플로잇 프레임워크 설계

상기 서술한 것과 같이, 보안 외장 하드 디스크에서 패스워드 노출과 같은 취약점으로 인하여, 사용자 인증 우회가 가능한 보안위협이 발생하므로, 이러한 취약점으로부터 보안 외장 하드디스크의 안전성을 점검하기 위하여, 본 논문에서는 보안 외장 하드디스크 취약점 익스플로잇 프레임워크를 제안하고 설계하였다.

설계한 프레임워크는 보안 프로그램을 프레임워크에 부착하여 취약점을 분석하는 기능을 제공하며, 패스워드, 지문, 키패드, NFC와 같은 각 제품에서 도입한 사용자 인증 방식에 따른 취약점 진단 기능을 제공한다. 또한, 최신의 새로운 취약점을 반영하기 위하여, 깃허브와 연동하여 익스플로잇 프레임워크를 업데이트하는 기능을 제공한다.

1. 익스플로잇 프레임워크 설계

본 절에서는 익스플로잇 프레임워크 설계와 관련된 전체 시스템 설계와 설계된 시스템에서 제공하는 각 기능 및 유즈케이스 다이어그램 설계 결과를 서술한다.

1.1. 전체 시스템 설계

본 논문에서 설계한 전체 시스템은 사용자, 보안 외장 하드디스크, 취약점 분석, 익스플로잇 프레임워크로 구성되며, 전체 시스템 설계 결과를 그림 3에 나타내었다.

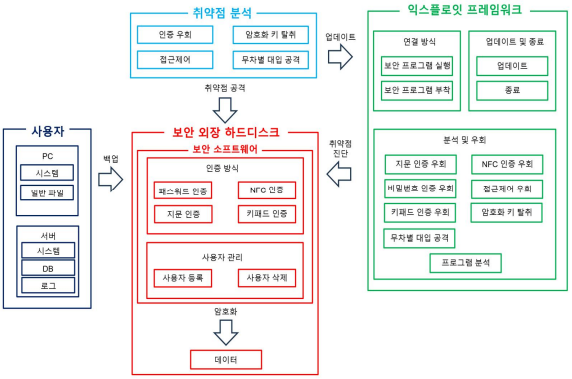

Fig. 3. 전체 시스템 설계도

사용자는 PC(Personal Computer)의 시스템 파일이나 일반 데이터, 서버의 시스템 파일이나 DB(DataBase), 로그 파일 등을 보관하기 위하여, 해당 파일들을 보안 외장 하드디스크에 백업한다. 백업하는 파일들은 외부에 노출되지 않아야 하는 데이터나 서버의 시스템 복구를 위한 백업과 같은 중요한 데이터이므로, 강력한 보안 수준이 요구된다.

보안 외장 하드디스크는 각 제품에서 도입한 인증 방식을 사용하여 사용자를 식별하며, 사용자를 관리하기 위한 기능으로, 사용자 등록 및 사용자 삭제 기능을 제공한다. 마지막으로, 사용자가 백업하는 데이터를 암호화하여 내부 저장소에 안전하게 저장한다. 그러나 이러한 보안 기능을 제공하더라도, 구현상의 문제점이나 설계상의 문제점과 같은 다양한 문제점으로 인하여, 취약점이 존재할 가능성이 있으므로, 취약점 분석이 요구된다.

취약점 분석은 보안 외장 하드디스크에서 발생 가능한 인증 우회, 암호화 키 탈취, 접근제어 취약점, 무차별 대입 공격과 같은 취약점을 분석하며, 분석 결과를 바탕으로, 익스플로잇 프레임워크에 반영한다. 더욱 다양한 취약점을 점검하기 위하여, 지속적으로 취약점을 분석하며, 발견된 취약점을 프레임워크에 업데이트한다.

익스플로잇 프레임워크는 분석 대상인 보안 프로그램의 연결을 위한 실행 및 부착 기능, 프레임워크의 업데이트 및 종료 기능, 프로그램의 분석 및 우회 기능을 제공한다. 프로그램의 분석 및 우회 기능은 프로그램의 내부를 분석한 후, 분석한 취약점을 바탕으로, 인증 우회, 암호화 키 탈취, 접근제어 우회, 무차별 대입 공격을 시도하고 그 결과를 출력한다. 이와 같이 본 논문에서 설계한 프레임워크를 기반으로 보안 외장 하드디스크의 취약점을 점검함으로써 안전성 평가가 가능하다.

1.2. 기능 설계

익스플로잇 프레임워크는 프로그램 연결 및 분석, 업데이트 및 종료, 다양한 취약점 진단 기능을 제공하며, 전체 기능 설계 결과를 그림 4에 나타내었다.

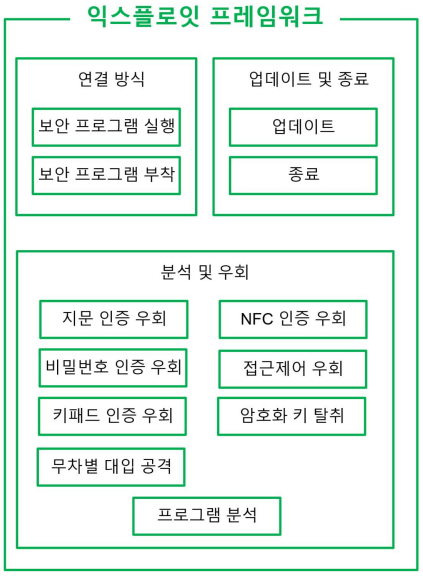

Fig. 4. 익스플로잇 프레임워크 기능 설계

- **보안 프로그램 실행 및 부착 기능:** 취약점을 분석할 보안 프로그램 실행한 후, 프레임워크에서 보안 프로그램으로 연결하거나, 프레임워크에서 이미 실행된 보안 프로그램에 부착하는 기능을 제공한다.
- **프로그램 분석 기능:** 취약점이 분석되지 않은 보안 프로그램을 대상으로, 발생 가능한 취약점을 분석함으로써 보안위협을 도출한다.
- **지문, 패스워드, 키패드, NFC 인증 우회 기능:** 지문, 패스워드, 키패드, NFC와 같은 사용자 인증 방식을 대상으로 보안 외장 하드디스크의 인증을 우회하는 기능을 제공한다.

● **암호화 키 탈취 기능**: 보안 프로그램이 데이터를 암호화하기 위하여 사용한 암호화키를 탈취하는 기능을 제공한다. 탈취한 암호화 키는 암호화된 데이터를 복호화함으로써, 비인가자가 원본 데이터를 획득하기 위한 정보로 활용한다.

● **접근제어 우회 기능**: 보안 프로그램에서 제공하는 접근제어를 우회함으로써, 비인가자가 파일이나 데이터와 같은 내부 자원에 접근하는 기능을 제공한다.

● **무차별 대입 공격 진단 기능**: 패스워드 인증 방식을 사용하는 보안 프로그램을 대상으로, 무차별 대입 공격이나 사전 대입 공격, 잘 알려진 공격과 같은 패스워드 탈취 기능을 제공한다.

● **업데이트 기능**: 깃허브를 통하여 프레임워크를 업데이트함으로써 새로운 취약점을 반영하는 기능을 제공한다.

1.3. 유즈케이스 다이어그램 설계

본 논문에서 제안하는 보안 외장 하드디스크 취약점 익스플로잇 프레임워크를 사용자의 관점에서 시스템의 서비스나 기능 및 외부 요소를 표현하기 위하여, 유즈케이스 다이어그램을 설계하였다. 'Creately' 도구를 사용하여 모델링 및 구조화, 상세화 단계에 따라 다이어그램을 작성하였으며, 그 결과를 그림 5에 나타내었다.

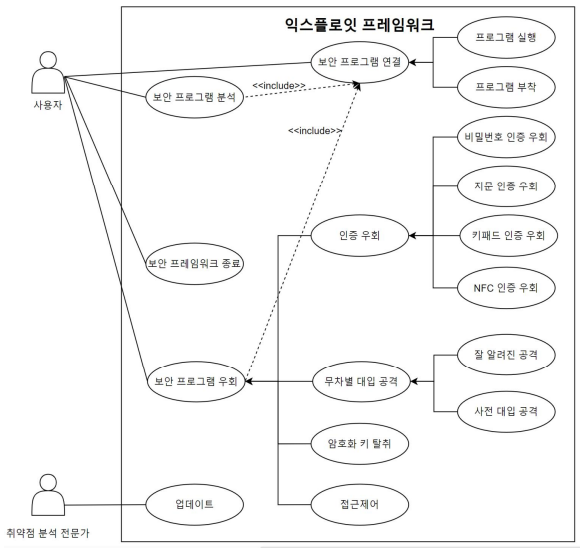

Fig. 5. 유즈케이스 다이어그램 설계

유즈케이스 다이어그램을 살펴보면, 액터로 사용자와 취약점 분석 전문가를 정의하였고, 유즈케이스는 보안 프로그램 연결, 보안 프로그램 분석, 보안 프로그램 우회, 보안 프레임워크 종료, 업데이트와 같은 사용자의 행위를 정의하였다. 포함 관계는 보안 프로그램 연결-보안 프로그램 분석 및 우회 관계를 정의하였고, 보안 프로그램 분석 및 우회를 진행하기 전, 보안 프로그램 연결이 선행되어야 한다. 일반화 관계는 보안 프로그램 연결-프로그램 실행 및 분석, 인증 우회-패스워드, 지문, 키패드, NFC 인증 우회, 무차별 대입 공격-잘 알려진 공격, 사전 대입 공격을 정의하였으며, 전자가 후자를 포함한다.

2. 프로토타입 설계

본 절에서는 설계한 프레임워크에 대한 프로토타입 설계 결과를 서술한다. 프로토타입을 설계하기 위하여, 프레임워크를 활용하는 시나리오를 도출하고, 도출된 시나리오에 따른 프로토타입 설계 결과를 서술한다.

2.1. 프레임워크 활용 시나리오

본 논문에서는 설계한 프레임워크를 활용하는 세 가지 시나리오를 도출하였다. 첫 번째 시나리오는 보안 개발자가 보안 외장 하드디스크의 안전성을 점검하는 것으로, 보안 외장 하드디스크의 보안 프로그램을 개발한 후, 프레임워크를 활용하여 보안 프로그램의 안전성을 점검함으로써, 개발한 프로그램에 내재된 취약점을 발견하고 이를 해결함으로써 보안성을 향상시킬 수 있다. 두 번째 시나리오는 일반 사용자나 기업의 보안 담당자가 보안 외장 하드디스크의 안전성을 점검하는 것으로, 사용자나 기업에서 사용할 샘플 보안 외장 하드디스크를 구매한 후, 프레임워크를 활용하여 안전성을 점검함으로써, 더욱 안전한 보안 외장 하드디스크를 선정하기 위한 목적으로 활용될 수 있다. 세 번째 시나리오는 한국인터넷진흥원 및 금융감독원과 같은 감독기관이 점검 대상 기업의 보안 진단을 실시하는 것으로, 프레임워크를 사용하여 보안 외장 하드디스크의 안전성을 검증할 수 있다.

2.2. 시나리오에 따른 프로토타입 설계

본 논문에서는 프로토타입을 설계하기 위하여, 첫 번째 시나리오를 선정하였고, 그 결과를 그림 6에 나타내었다.

설계한 프로토타입은 프레임워크를 통하여 수행 가능한 기능을 상세하게 설계한 것으로, 각 기능을 설명하면, 사용자가 PC에 보안 외장 하드디스크를 연결하고 보안 프로그램을 실행시키는 경우에는 프로그램 열기나 프로그램 부착 기능을 활용하여 보안 프로그램을 익스플로잇 프레임워크로 연결하고, 인증, 접근제어 우회, 암호화 키 탈취, 무차별 대입 공격과 같은 다양한 공격을 시도함으로써 발생 가능한 취약점을 진단한다. 또한, 업데이트 기능을 활용하여 프레임워크를 최신으로 업데이트하며, 종료 기능을 통하여 프레임워크를 종료시킨다.

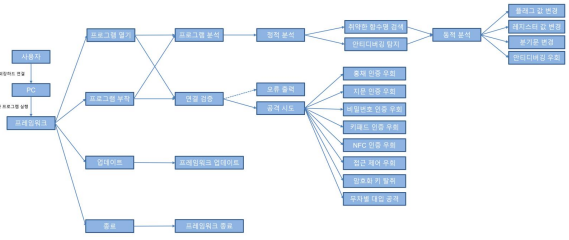

Fig. 6. 프로토타입 설계

2.3. UI 설계

설계한 프로토타입을 기반으로, 익스플로잇 프레임워크 UI(User Interface)를 설계하였으며, 그 결과를 그림 7에 나타내었다.

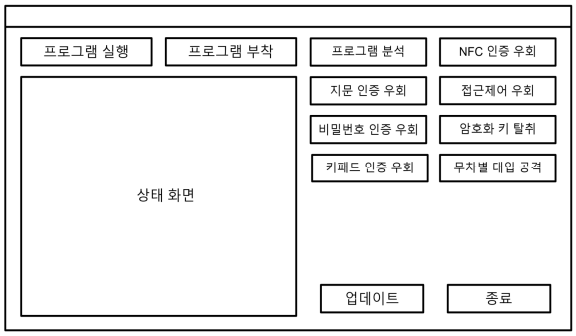

Fig. 7. UI 설계

설계한 각 기능을 버튼을 통하여 제공함으로써, 사용자가 직관적으로 사용하도록 UI를 설계하였으며, 제공되는 각 기능 및 상태, 실행 결과를 상태 화면에 출력함으로써, 취약점 진단 결과를 사용자가 확인하도록 설계하였다.

Ⅳ. 결론

보안 외장 하드디스크는 일반 외장 하드디스크에 보안 기능을 추가함으로써, 안전성을 향상시켰지만, 인증 우회 및 암호화 키 노출과 같은 취약점으로 인하여, 비인가자로부터 디스크 내부에 안전하게 저장된 데이터가 탈취되는 보안위협이 발생하였다. 본 논문에서는 이러한 취약점을 점검하기 위한 목적으로 보안 외장 하드디스크 취약점 익스플로잇 프레임워크를 제안하고 설계하였다. 설계한 프레임워크는 보안 외장 하드디스크의 보안 프로그램을 분석하고, 보안 외장 하드디스크에서 제공하는 인증 방식에 따른 인증 우회, 암호화 키 탈취, 무차별 대입 공격, 접근제어 우회 취약점을 진단하는 기능을 제공하며, 새로운 취약점을 반영할 수 있도록 업데이트 기능을 제공한다.

본 논문에서 설계한 프레임워크를 활용한다면, 현재 상용화된 보안 외장 하드디스크나 추후 개발될 보안 외장 하드디스크를 대상으로 더욱 편리하게 안전성을 평가할 수 있으며, 평가 결과를 기반으로, 보안 외장 하드디스크에 내재된 취약점을 보완함으로써 안전성을 더욱 향상시킬 것으로 판단된다.

향후, 설계한 보안 외장 하드디스크 취약점 익스플로잇 프레임워크의 기능 및 사용성과 같은 설계를 더욱 보완하고 프레임워크를 개발함으로써, 상용 보안 외장 하드디스크를 대상으로 발생 가능한 취약점을 점검할 예정이다.

ACKNOWLEDGEMENT

본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 자원을 받아 수행된 지자체-대학 협력기반 지역 혁신 사업의 결과입니다(2023RIS-1345370809).
본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.(2021RIS-002)

REFERENCES

[1] A. M. Salma and B. Walaa, "A dynamic model of viruses with the effect of removable media on a computer network with heterogeneous immunity," Advances in Difference Equations, pp. 1-20, Jun. 2020.

[2] O. Kyle, S. C. David, A. D. Striegel, and C. Poellabauer, "Power and performance characteristics of USB flash drives," IEEE International Symposium on World of Wireless Mobile and Multimedia Networks, pp. 1-4, Jun. 2008.

[3] D. Ashish, G. Vishal, and S. Damanbir, "Secure Portable Storage Drive: Secure Information Storage," International Conference on Communication, Networks and Computing, pp. 308-316, Oct. 2018.

[4] Z. Liu, K. Hao, Y. Zhang, and X. Niu, "The Design of Smart Fingerprint Portable Storage Device with Encryption Function," Citeseer, *https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=fafc92d7a1aefa765df808ace439091f5a5fa67d*, accessed on December 27, 2023.

[5] S. Kwak, S. Go, J. Lee, J. Lee, J. Yun, and K. Lee, "Vulnerability Analysis and Demonstration of Fingerprint Authentication in Secure USB Drives: Based on Product F," Proceedings of the Summer Conference on the Korea Society of Computer Information, Vol. 31, No. 2, pp. 189-190, Jul. 2023.

[6] J. Lee, D. Kim, W. Jung, and K. Lee, "Vulnerability Analysis of Secure External Hard Drives: Based on the Password Authentication of Product B," The 15th Workshop on Convergent and Smart Media Systems, pp. 1-3, Feb. 2023.

[7] H. Kim, S. Lee, and I. Lee, "Design and Implementation of Security Solution for Potable Hard Disk Drive," Proceedings of the Spring Conference on the Korea Multimedia Society, Vol. 13, No. 1, pp. 50-53, May 2010.

[8] National Cyber Security Center, "Security Requirements for Software-based Secure USB products," *https://www.ncsc.go.kr/*, accessed on December 19, 2023.