기술정보 유출방지를 위한 보안저장매체 연구
(스마트카드/생체정보 인증기반)

김 도 경
고려대학교 컴퓨터정보통신대학원
e-mail: kdk0724@korea.co.kr

A Study on the Security Storage Device for the Prevention from Technical Assets Outflow
(Smart Card/Biometric-Based Authentication)

Do Kyoung, Kim
Graduate School of Computer & Information Technology, Korea University

요 약

대부분 기업의 중요 기술정보 유출은 내부자에 의해 이루어진다. 기업의 핵심기술 및 정보유출을 방지하기 위하여 여러 분야에서 많은 투자와 연구가 진행되고 있지만 기술발전에 따라 업무환경과 일하는 방법이 변화하여 물리적보안과 정보보안을 분리한 기존 개별 통제방식은 효용성이 떨어지고 있다.

새로운 환경에 대응하기 위하여 보안 패러다임의 전환이 필요한 시점이다. 이에 본 연구는 물리적보안과 정보보안을 융합한 신뢰할 수 있는 인증기반(스마트카드/생체정보) 보안저장매체의 요구기능, 각 기능에 필요한 요소기술에 대하여 고찰한다.

1. 서론

IT기술발전과 기업생태환경(Business Ecosystem) 변화에 따라 기업의 자산의 속성, 일하는 방법, 업무환경이 비정형화 되고 유동적인 구조로 진화하고 있다.

유형의 물리적 자산에서 무형의 정보자산 중요성이 증가하고, 글로벌 수준의 협업과 재택근무, 모바일 업무 등이 활발해지면서 외부저장매체를 이용한 업무의 필요성이 증대하나 일률적인 보안통제정책으로 불편을 초래하고 있다.

소형의 비금속재질인 보조기억장치(USB 등)는 기업이 정보보안을 위해 운영하고 있는 물리적인 검색시스템(X-Ray, 금속탐지기)으로 검출이 어려우며 외부저장매체 사용을 인가하면, 과다한 정보반출 및 반출 후 사용 추적관리가 불가능하다.

또한, 급증한 정보량과 유통경로의 다양화로 물리적 보안 및 정보보안의 분리된 기술과 통제방법으로는 적절한 보안통제가 현실적으로 어려움이 있고, 보안통제기술과 방법은 기술발전추세와 환경변화에 대응이 늦어 정보유출을 통제하기에는 미흡하다. 그래서 글로벌화 되는 업무환경에 대응하여 보안은 강화하고 업무편의성을 보장 할 수 있는 스마트카드/생체정보(지문) 인증기반 보안저장매체에 관한 연구를 시작하게 되었다.

2. 관련연구

2.1 스마트카드/생체 인증기반 보안저장매체 개요

최근 기업들은 대부분 물리적 접근통제를 하기위해 출입통제시스템과 출입증 용도로 스마트카드 사원증을 패용하며, 인가된 사람만 출입을 할 수 있는 시스템을 구축하여 운영하고 있다.

본 논문은 물리적 보안 Infra가 구축된 기업 또는 중요정부기관에 대하여 스마트카드/생체정보(지문) 인증기반 보안저장매체(이동형 HDD 등)를 이용하여 대량의 불법 정보유출을 통제/추적관리하기 위한 연구이다.

2.2 연구모델 및 가정

국정원에서는 '보조기억매체'라 함은 디스켓, 이동형 하드디스크(HDD), USB메모리, CD, DVD 등 자료를 저장할 수 있는 일체의 것으로 PC등의 정보통신시스템과 분리할 수 있는 기억장치를 말한다.

대부분 기업 또는 중요 정부기관에서는 PC보안프로그램(에이전트)을 이용하여 '보조기억매체' 사용을 통제하고 있다. 단, 업무 성격상 부득이한 경우 보안정책으로 보조기억매체를 사용하고 있다.

연구의 전제조건은 인가된 보안저장매체는 PC보안 프로그램(에이전트)으로 사용허가를 가정한다.

2.3 기술동향

본 논문에 언급되었던 보안저장매체와 유사한 기술로 분류되는 보안USB 관련 동향을 살펴보도록 한다.

국정원은 "USB등 보조기억매체 보안관리지침('07.01)"제정 발표하였으며, 중앙행정기관(대통령 소속기관 및 국무총리 소속기간을 포함) 및 지방자치단체 및 소속·산하기관(이하 "각급기관")에 의무도입('08. 4부터)을 규정하여 현 수준은 확산 단계라고 볼 수 있다.

국가정보원장은 보안적합성 검정 시 다음 각 호에 해당하는 필수 보안기능의 유무를 검토 한 그 결과를 적합성 검증결과에 반영한다.

① 사용자 식별·인증기능
② 저장데이터 암·복호화 기능
③ 저장된 자료의 임의 복제 방지기능
④ 분실시 저장데이터의 보호를 위한 삭제 기능

관련 업계 기술수준을 살펴보면 8개사가 국정원에서 제정하여 발표한 "USB등 보조기억매체 보안관리지침"요구기준에 충족하는 기술을 보유하는 업체들이다.

<표1> 국정원 보안USB 검정필제품 현황

제품명	보안USB 관리시스템 V1.4			
개발사	제품군	검증일	검증등급	참고사항
비트비솔루션(주)	보안USB	20090219	-	
제품명	nProtect UMS V1.0			
개발사	제품군	검증일	검증등급	참고사항
(주)잉카인터넷	보안USB	20081230	-	
제품명	nTracker USB Enterprise Edition V3.1			
개발사	제품군	검증일	검증등급	참고사항
엠로텍커(주)	보안USB	20080415	-	
제품명	USB Management System			
개발사	제품군	검증일	검증등급	참고사항
(주)아이티넷이도	보안USB	20080407	-	
제품명	IGM-Public 2.0			
개발사	제품군	검증일	검증등급	참고사항
(주)솔루션어소시에이트	보안USB	20080407	-	
제품명	SafeUSB+ V1.1			
개발사	제품군	검증일	검증등급	참고사항
(주)넥스터즈	보안USB	20080407	-	
제품명	FX-USB V1.0			
개발사	제품군	검증일	검증등급	참고사항
(주)테크로아	보안USB	20080218	-	
제품명	UToken combo 유			
개발사	제품군	검증일	검증등급	참고사항
(주)칼텍시스	보안USB	20071228	-	

이와 같은 업계에서는 USB 저장매체를 기반으로 불법 정보유출을 통제하는 솔루션을 보유하고 있다.
보안저장매체 용도로 상용화 된 USB메모리 저장용량은 1G, 2G, 4G, 8G 정도로 이동형 하드디스크(HDD)에 비해 비교적 작은 저장용량이다.

3. 고려사항

산업기술보호법으로 보호되는 기업 및 중앙행정기관(이하 "각급기관") 등의 기관들이 보유한 중요 정보자산들(DRM 문서, 도면, 3D 설계자료 등)은 수GByte부터 수십 GByte에 이르기에 급증한 정보량을 대비하여 본 연구에 적용한 보안저장매체는 외장형하드디스크(HDD)로 적용하기로 한다.

스마트카드/패스워드 인증은 도용이나 불법취득에 의한 사용시 큰 혼란에 빠지게 된다.

"철수가 진짜 철수인지" 인증에 대한 무결성을 확보하기 위하여 개인 식별기술이 생체인식으로 신뢰할 수 있는 인증이 되어야 한다. 개인정보/생체정보 데이터 송수신에도 암호화된 통신 네트워크를 이용하여 중간에 불법적인 접근을 막아야 한다.

생체정보 인증에 관련된 Traffic용량과 개인정보(지문)유출 등의 사유로 식별된 생체정보를 원격에 위치한 서버에서 보유하고 있는 데이터 비교를 통하여 인증하는 방법은 비효율적으로 판단된다.

이를 보완하기위해 스마트카드 Reader와 생체인증(지문) 디바이스를 보안저장매체에 탑재하여 스마트카드에 지문정보를 저장하고 생체인식 디바이스에 의해 인식된 생체정보를 비교한 결과를 가지고 원격에 있는 서버에 인증을 받는 구조를 설계하였다.

3.1 핵심 요구기능의 정의

앞서 서술 되었던 보안USB 기술동향을 검토한 결과 산업기술보호법으로 보호되는 기업과 높은 보안등급을 요구하는 기관에서 요구하는 기능을 아래와 같이 정의 하였다.

<표2> 보안저장매체 요구기능 정의

사용자 인증	컨텐츠 사용제어
· 사원증 정보탑재 (생체정보/I-PIN) · 저장매체 스마트카드 인식리더/생체인식 디바이스 탑재 · 사용자 정보 매칭	· 데이터 사용/접근 권한관리 - 저장/검색 - 읽기/수정 - 분배/출력 - 컨텐츠 재생산
컨텐츠 보호	**N/W접근제어**
· 암호화 저장/보관 · 복호화 사용	· N/W 접근권한 차등관리 - 사내망/ 사외망
원격제어/추적관리	**자산관리**
· 분실자료 원격삭제 (N/W 접속탐지 시) · 사용현황 Log 추적 · 보안정책 설정/변경	· 반출/반입 등록/관리 · 비인가 반출탐지

4. 스마트카드/생체 인증기반 보안저장매체 Framework

3절에서 요구기능을 분석한 결과 필요한 요소기술에 대하여 자세히 살펴보도록 하겠다.

<표3> 보안저장매체 요소기술 정의

개인정보 인증/관리기술	매체운영 기술
· 스마트카드 기술 · 생체인식 기술 · 개인정보 보호 · 개인정보인증 (I-PIN/생체정보)	· 접근제어기술 (정책제어/관제) · 컨텐츠 보호기술 · 사용자 인증기술
컨텐츠 권한관리 기술	**컨텐츠 보호기술**
· 사용자 인증/추적 · 컨텐츠 권한관리 (사용제어) · DRM 상호호환	· 암호화/복호화 · 암호 알고리즘
네트워크 보안기술	**정보유출방지 기술**
· 사용자 인증/추적 · 컨텐츠 권한관리 (사용제어)	· 모니터링 기술 (Data, N/W, 장치) · 전자파기 기술
	자산관리 기술
	· RFID 기술

4.1 개인정보 인증/관리 기술

스마트카드/생체정보 인증기반 보안저장매체에서 가장 중요한 요소기술이다. 아래에 제시한 여러 요소기술들도 중요하지만 신뢰할 수 있는 인증을 하여야 한다.

직원들이 보유한 스마트카드에 생체정보를 탑재하여 단말기에 탑재된 생체정보의 데이터를 비교하여 정당한 본인임을 확인하는 기술이다.

☞ 스마트카드 기술

보안저장매체에 스마트카드 인식기술이 탑재하여 스마트카드를 통한 개인인증이 가능하여야 하며 임의복제가 불가능한 암호화된 포맷으로 관리가 되어야 한다.

☞ 생체인식 기술

보안저장매체에 지문인식기술이 탑재되어 생체정보로 정당한 개인을 식별 할 수 있어야 한다.

☞ 개인정보 보호

특정개인을 식별하거나 식별할 수 있는 일체의 정보를 보호 할 수 있도록 한다.

☞ 개인정보 인증

정당한 개인을 식별할 수 있는 수단을 제공하여야 한다.

4.2 매체운영 기술

매체 운영이라 함은 지정된 매체에 대해서만 내부사용을 가능하도록하고 외부 사용 시에는 지정된 보안정책 환경 내에서 사용하도록 통제하는 것을 의미한다.

☞ 접근제어

중앙관리 서버를 통하여 사용자의 저장매체 사용을 통제 및 관제하고 사용자 및 장치에 대한 개별관리를 수행하며, 관리대상에 대한 보안정책을 부여 할 수 있도록 한다.

☞ 컨텐츠 보호

저장매체에 저장된 컨텐츠를 보호하기위해 제공되는 DRM 솔루션과의 연동구조를 확보한다.

이러한 연동구조는 장치별로 생성되는 고유정보 또는 생성 키값에 기준하여 연동 할수 있는 구조이다.

☞ 사용자 인증

저장매체 사용을 위한 사용자 인증 수단을 제공한다.

4.3 컨텐츠 권한관리기술

보안저장매체에 기록된 컨텐츠는 사용자 권한 또는 중앙관리서버 정책에 따라 차등관리에 대한 기능을 의미하며 비인가자에 의한 접근 및 훼손을 방지하기 위한 기능을 제공한다.

☞ 사용자 인증/추적

컨텐츠 사용자 인증을 수행하고 컨텐츠 사용자에 대한 이력 추적관리가 가능한 구조를 수립한다.

☞ 컨텐츠 권한관리

컨텐츠의 보안등급에 따라 읽기전용, 수정 등의 사용제어가 가능하여야 한다.

☞ DRM 상호호환

DRM 솔루션에서 독립적으로 사용할 수 있는 고유정보 또는 키관리 공간을 매체에 제공하고 이 공간을 네트워크 서버를 통하여 관리 할수 있도록 한다

4.4 컨텐츠 보호기술

보안 저장매체에 저장되는 컨텐츠는 암호화 알고리즘에 의해 암/복호화 되어 비인가자 접근에 대한 컨텐츠를 보호하여야 한다.

☞ 암호화/복호화

보안저장매체에 컨텐츠 저장 시 암/복호화 기능으로 컨텐츠가 보호되어야 한다.

☞ 암호 알고리즘

암호 알고리즘은 안전성을 기반으로 비밀성과 무결성이 보장되어야 한다.

4.5 네트워크 보안기술

네트워크 보안이라 함은 내외부 환경에서의 매체 사용시 이를 네트워크를 통하여 제어 및 통제하는 것을 의미한다. 네트워크 보안에서 제공되는 요소기능은 다음과 같다.

☞ 사용자 인증

네트워크 서버인증을 통하여 사용자 인증을 수행하고 장치에 대한 사용을 허가하는 구조를 수립한다.

☞ 사용자 추적

IP또는 MAC 정보에 기반하여 사용자를 추적할 수 있는 기능을 제공하고 이에 대한 로그정보를 수집한다.

☞ 컨텐츠 권한관리

DRM 솔루션과 연동하여 네트워크 인증을 수행할 수 있는 구조를 수립한다. 이는 매체운영의 컨텐츠 보호를 위한 구조와 연동되는 기능이다.

4.6 정보유출방지

정보유출방지라 함은 저장매체에 기록된 자료들에 대한 감시 및 부정사용 또는 비인가자의 불법도용 시도 시 자료파괴에 대한 통제를 의미한다.
정보유출방지에서 제공되는 요소기능들은 다음과 같다.

☞ 데이터 사용감시

실시간 데이터 사용로그를 기록하고 이를 서버전송 또는 저장매체 내에 저장하여 중앙관리서버에 사후 전송할 수 있도록 한다.

☞ 네트워크 환경감시

사용자 PC의 네트워크 환경인 IP 또는 MAC에 대한 정보를 추출하고 이에 대한 사용여부를 통제한다.

☞ 장치 사용감시

장치 사용 시도시 이에대한 인증로그를 수집하여 사용자의 장치사용에 대한 감시를 수행한다.

☞ 원격데이터 파괴

비인가 환경내에서의 사용 또는 분실장치 등에 대하여 원격에서 저장된 데이터를 삭제할 수 있는 기능을 제공한다.

4.7 자산관리 기술

자산관리라 함은 반출/반입등록 관리가 이루어져야하며 비인가자 무단반출을 탐지하여 이상신호를 중앙관리서버로 전송하여야 한다.

☞ RFID기술

무선인식 기술을 적용하여 보안저장매체가 비인가 반출 시도를 탐지하여 중앙관리서버로 이상신호를 전송하여야 한다.

5. 결론

스마트카드/생체정보 인증기반 보안저장매체는 기업 및 중요정부기관의 핵심기술정보 유출방지를 목적으로 연구하여 보안성은 높으나, 암/복호화에 소요되는 시간, 속도 등의 가용성과 여러 운영 체제에서도 안정적인 동작을 할 수 있는 범용성에 대한 검토가 필요하다

또한 스마트카드 Reader 안테나 설계와 지문인식 모듈탑재 등도 보안저장매체 소형화/실용성도 중요한 요소가 될 것이다.

신뢰성과 범용성, 가용성이 확보 된다면 물리적보안과 정보보안을 융합 함으로서 정보시스템 등에 대한 싱글사인온(Single Sign On)과 권한 권리(EAM, Extranet Access Management) 등 다양한 응용분야에 서비스 확대가 예상된다.

참고문헌

[1] USB 메모리 등 보조기억매체 보안관리 지침, 2007
[2] 산업자원부고시 제2007-109호, 2007
[3] 기술유출 방지를 위한 정보시스템 보안방향
[4] RFID를 이용한 복합기 보안시스템, 2007
[5] 연구정보 보안강화 방안
[6] 국가정보보호백서, 2008