韓國컴퓨터情報學會 論文誌
第16卷 第4號, 2011. 04.

2011-16-4-3-1

이중사용 방지를 위한 USB 보안 프레임워크의 설계

정 윤 수*, 이 상 호**

Design of an USB Security Framework for Double Use Detection

Yoon-Su Jeong*, Sang-Ho Lee**

요 약

최근 인터넷 기술의 발전으로 인하여 사용자의 개인정보가 USB에 저장되어 사용되고 있지만 USB에 저장되어 있는 개인정보는 별도의 사용자 인증 과정이 필요없어 악의적인 목적으로 사용되어 개인정보가 노출될 수 있는 문제가 있다. 이 논문에서는 USB에 저장되어 있는 개인정보를 보호하기 위해서 개인정보의 이중사용 방지를 위한 USB 보안 프레임워크를 제안한다. 제안된 USB 보안 프레임워크는 서로 다른 네트워크에서 USB 보안 제품을 사용할 경우 USB 보안 토큰의 사용 유·무 및 사용자의 속성 정보를 인증 정보 앞에 추가하여 사용자의 인증 과정을 수행하기 때문에 통신 오버헤드 및 서비스 지연이 향상되었다. 실험 결과 단순파일 저장매체(USB driver)와 자체 연산 가능한 매체(USB Token) 보다 제안된 USB 보안 프레임워크가 패킷 인증 지연시간에서 평균 7.6% 향상되었고, USB수에 따른 인증서버의 처리량에서도 평균 9.8% 향상된 결과를 얻을 수 있었다.

▸ 키워드 : 보안 프레임워크, 인증, 이중사용

Abstract

Recently, the development of internet technology makes user's personal data used by being saved in USB. But there is a critical issue that personal data can be exposed with malicious purpose because that personal data doesn't need to be certificate to use. This paper proposes USB security framework to prevent a duplicate use of personal data for protecting the data which in USB. The proposed USB security framework performs certification process of user with additional 4bite of user's identification data and usage choice of USB security token before certification data when the framework uses USB security product in different network. It makes communication overhead and service delay increased. As a result of the experiment, packet certification delay time is more increased by average 7.6% in the proposed USB security framework than simple USB driver and USB Token, and procedure rate of certification server on the number of USB is also increased by average 9.8%.

• 제1저자 : 정윤수 • 교신저자 : 이상호
• 투고일 : 2010-11-12, 심사일 : 2010-12-23, 게재확정일 : 2010-12-27
* 한남대학교 산업기술연구소 전임연구원(Industry Technical Research Institute, Hannam University)
** 충북대학교 전자정보대학 소프트웨어학과 교수(Dep. Computer Science, College of Electrical & Computer Engineering, Chungbuk National University)
※ 이 연구는 2010년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음.

▸ Keyword : Security Framework, Authentication, Double Use

Ⅰ. 서 론

정보화 사회가 진행됨에 따라 기업의 기술, 영업 비밀 또는 개인의 민감한 데이터 파일을 정확하고(무결성) 안전하게(기밀성) 관리하는 기술의 중요성이 부각되고 있지만 정보의 도용, 남용, 해커, 불법 접근 등 정보화 사회의 역기능은 계속 증가하고 있다. 이에 과거 국방 등에 한정되어 사용하던 암호 기술을 기업 정보나 주요 공공 정보, 상거래 정보, 그리고 개인의 프라이버시 보호를 위해 사용되어지고 있다. 네트워크 환경에서의 PC 또는 Workstation은 해커 또는 바이러스로부터 결코 안전할 수 없다. 따라서 물리적으로 안전한 영역(TCB: Trusted Computing Base) 에서의 암호 알고리즘 수행과 사용자 키의 관리가 요구된다. 또한 사용자의 키는 개별적으로 관리하는 것이 위험을 분산시킬 수 있으며 이러한 관점에서 보안 토큰은 차세대 정보보호의 가장 중요한 영역이 되고 있다.

보안토큰은 사용자 인증을 위한 용도로 IC칩을 탑재해, 정보를 기록/처리할 수 있도록 하고 있으며, USB 플로그 형태를 한 USB형 토큰 등이 주로 사용된다. USB형 토큰 제품은 크기가 작아 휴대가 간편하고, 데이터의 입출력 속도는 최대 480Mbit/s로 기존에 사용하던 플로피 디스켓이나 ZIP 드라이브와 비교할 수 없을 정도로 빠르다. 이러한 이유로 USB 보안토큰 제품은 작은 크기의 문서 파일이나 공인인증서의 저장 등의 역할에만 머무는 것이 아니라 대용량 파일 전송이나 보관, 운영체제의 부팅 디스크 역할, PC 복구 등 다양한 역할을 수행할 수 있다.

그러나 USB 보안토큰 제품은 크기가 작고 대용량의 파일을 빠르게 전송할 수 있는 점을 이용하여 회사의 기밀을 유출하는데 이용하기도 하며, 다수의 PC 및 모바일 기기와 연결되는 특징을 이용하여 악성 코드나 바이러스, 웜 등의 유포에도 기여한다. 또한 사용 중인 USB 플래시 드라이브를 분실하면 습득자에게 저장되어 있는 모든 정보가 누출될 수 있고 개인적인 각종 문서 및 음악, 동영상 파일 등이 악용될 수 있다.

이와 같은 문제를 해결하기 위해서는 초기에 USB 보안토큰 제품에 비밀번호를 설정할 때, 사용자에게 입력받은 비밀번호를 해쉬함수를 이용하여 해쉬값을 이중으로 생성하는 저장 방법이 필요하다. 특히, USB 보안토큰 제품을 복제하여 기업이나 주요 공공 기관의 내·외부에서 USB 보안토큰 제품을 이중으로 사용할 경우, 사용자에게 입력받은 비밀번호의 무분별한 사용은 민감한 정보의 유출을 발생시키기 때문에 USB 토큰 제품의 이중 사용을 방지하기 위해서 USB 토큰 제품을 관리하는 관리서버는 USB 보안토큰 제품의 정보를 이용하여 USB 보안토큰 제품의 이중사용 여부를 알아낼 수 있는 보안 프레임워크가 필요하다.

이 논문에서는 USB 보안 토큰 제품의 이중사용을 예방하기 위해서 USB 보안 토큰 제품이 비밀번호를 설정할 때 사용자에게 입력받은 비밀번호와 속성정보를 이용하여 USB 보안토큰 제품의 이중사용을 예방하는 보안 프레임워크를 제안한다. 제안된 보안 프레임워크는 특정 장소에서 사용자가 USB 보안 토큰 제품을 사용할 때 USB 보안 토큰의 사용 유·무 및 사용자의 속성 정보만을 이용하여 인증 과정을 수행하기 때문에 통신 오버헤드 및 서비스 지연과 같은 통신 장애가 최소화된다.

이 논문의 구성은 다음과 같다. 2장에서는 USB 토큰 및 USB 보안 취약점에 대해서 분석한다. 3장에서는 USB 에 저장되어 있는 개인정보의 이중 사용을 예방하기 위한 USB 보안 프레임워크를 제시하고, 4장에서는 제안 기법에 대한 성능 평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련연구

2.1 USB 토큰

USB(Universal Serial Bus) 토큰은 (그림 1)과 같이 USB 호스트와 USB 토큰으로 구성된다. USB 호스트는 입력장치와 입력장치로부터 수집된 정보를 암호처리하는 시스템, USB 토큰으로부터 데이터를 전송하는 USB 마스트를 포함한다. USB 토큰은 호스트로부터 전달받은 암호화 데이터로부터 정보를 추출하는 암호처리와 정보를 저장하는 메모리, 데이터를 이용하여 인증을 수행하고 출력하는 CPU 그리고 USB 슬레이브를 포함한다.

(그림 1)의 USB 토큰은 사용자 등록과정과 인증과정으로 구분하며 사용자 등록과정에서는 사용자의 개인정보를 암호화한 후 USB 디바이스를 이용하여 메모리에 저장하는 과정을 의미하며 사용자 인증과정은 입력장치를 이용하여 사용자의 정보를 전처리 및 추출과정을 통해 메모리에 저장된 토큰 정보와 매칭하여 인증결과를 출력하는 과정을 의미한다.

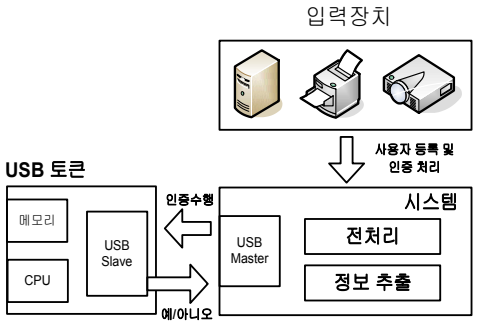

그림 1. USB 토큰 처리 시스템
Fig 1. USB Token Process System

USB 토큰은 전자주민증, 기업 신분증 등의 신분증, 전자화폐, 홈뱅킹, 인터넷 및 이동통신 단말기를 이용한 전자상거래 등의 금융 및 증권, 국가기간 전산망 접근통제, PC 보안, 휴대폰 가입자 확인 등의 네트워크, 의료보험증, 건강진단카드 등의 의료 분야 등에 사용된다.

2.2 USB 보안 취약점

USB 메모리는 일반적으로 USB 포트에 접속하여 사용하기 때문에 별도의 사용자 인증 과정이 필요없어 악의적인 목적으로 타인이 취득하게 될 경우 USB 메모리에 있는 모든 데이터가 노출되어 큰 피해를 입을 수 있다. 이중 가장 심각한 취약점은 VMWare 설치 취약점으로써 PC에 설치돼 있는 보안 USB 에이전트를 무력화할 필요없이 단순하게 VMWare 소프트웨어만 설치하면 누구나 내부의 중요 자료를 손쉽게 저장하거나 유출할 수 있고 사용 로그조차 남지 않기 때문에 상당히 위험한 취약점으로 나타났다. 그 외 USB 보안 취약점으로는 특정 SW를 통한 보안USB 영역 직접 액세스해 데이터 읽기 및 복사가 가능한 취약점과 안전모드 부팅 후 보안USB 폴더를 삭제해 무력화 시키는 취약점 등이 있다. 그리고 보안 USB 실행파일을 강제 종료 후 일반 USB로 중요 내부 자료를 유출할 수 있는 취약점과 공인(사설)인증서 저장시 보안 USB에서 예외처리되는 것을 악용해 내부 자료를 인증서 확장자로 변환해 저장 후 유출할 수 있는 취약점 등도 있다. 또한 PC부팅시 보안 USB 프로그램이 실행되기 전 시간을 이용해 일반 USB로 중요 자료를 유출할 수 있는 취약점도 최근 사용자에게 많은 피해를 주고 있는 것으로 나타났다. 이 같은 USB 보안 취약점들을 예방하기 위해서는 서버관리 프로그램을 통해서 USB가 접속할 때마다 서버 관리 프로그램에 등록된 USB만이 접속하도록 관리하여야 한다.

III. USB 이중 사용을 예방하기 위한 USB 보안 프레임워크

이 장에서는 USB의 이중사용 여부를 체크하기 위한 비트를 사용자의 인증 정보에 추가하여 사용자의 개인정보를 보호하기 위한 USB 보안 프레임워크를 제안한다. 제안된 USB 보안 프레임워크는 USB 마스터와 USB 슬레이브 사이에 논리적으로 동작하는 에이전트를 두어 USB 드라이버의 인스톨 파일을 사전에 저장하여 도청 행위 공격을 사전에 예방한다. 또한, USB 보안 프레임워크에서는 플러그 앤 플레이 기능이 수행될 때 USB 슬레이브와 USB 마스터에서 생성한 랜덤 수를 이용하여 보안 토큰을 생성한다.

3.1 개요

USB 장치에 저장되어 있는 사용자의 개인정보는 인증 과정없이 네트워크에서 악의적인 목적으로 사용될 수 있기 때문에 USB 장치내에 저장되어 있는 사용자 정보의 이중사용 여부를 서버가 체크하여 USB 장치내에 저장되어 있는 개인정보를 보호할 필요가 있다. 제안된 보안 프레임워크에서는 USB 장치내에 저장되어 있는 사용자 정보의 이중사용 여부를 파악하기 위해서 USB 장치를 USB 마스터와 USB 슬레이브로 구분하여 보안 기능을 수행한다. (그림 2)는 USB 장치가 USB 보안 관리 에이전트와 USB 보안 에이전트로 구성된 제안된 USB 보안 프레임워크의 개념도를 보여주고 있으며 (그림 2)에서 USB 장치는 USB 마스터와 USB 슬레이브가 직접적으로 USB 포트를 사용하여 연결되고 있음을 가정한다.

(그림 2)에서 제안된 보안 프레임워크는 USB 토큰, USB 리더, 인증 서버로 구성되며 USB 토큰은 사전에 등록된 USB PIN 정보를 USB Token의 메모리에 저장하고 USB 리더는 USB 토큰을 인식하는 USB 보안 관리 에이전트 모듈과 키를 저장하는 Key-storage, 메시지를 암·복호하는데 사용되는 PKI 생성 알고리즘 등이 동작한다. USB 토큰을 사용하는 사용자들은 USB 리더의 통신 범위를 벗어날 경우 일정 시간이 경과한 후 인터럽트가 발생하여 통신을 중지한다.

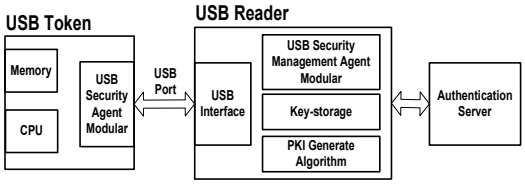

그림 2. 제안된 보안 프레임워크의 인터페이스
Fig 2. Interface of Proposed Security Framework

사용자의 개인키와 USB Token의 랜덤키에 의해서 동작되는 해쉬 과정은 USB 리더를 통해 수행되며 USB 인터페이스를 통해 키와 데이터 정보들을 사전에 인증 서버에 저장된 정보들과 서로 교환한다. 인증서버는 다중 사용자의 공개키를 저장하고 있어 MCU(Micro Control Unit)로부터 PIN을 체크하고 해쉬 결과로부터 랜덤 코드를 검색한 후 검색된 코드를 인증 서버가 보유하고 있는 정보와 비교하여 두 결과가 일치한다면 사용자의 개인정보의 이중사용 없이 인증이 성공적으로 이루어지고 그렇지 않으면 에러 정보를 전달한다.

3.2 USB 보안 프레임워크 구성요소

USB 보안 프레임워크는 USB 보안 관리 에이전트와 USB 보안 에이전트로 구성된다. USB 보안 관리 에이전트는 다양한 모델의 USB 보안을 관리해주는 역할을 하고 USB 보안 에이전트는 USB 리더와 주고받는 메시지를 처리하는 역할을 담당한다. USB 보안 관리 에이전트는 다양한 모델의 USB 보안을 관리하기 위해서 환경설정, 보안 USB 정보 조회, 메모리 영역 관리, 보안 USB 에이전트 저장, 보안 USB 에이전트 초기화, 보안 USB 에이전트 해제, 공통 보안 USB I/F 등의 역할을 수행하는 기능들로 구성된다. USB 보안 에이전트는 통신과 메시지 처리 모듈은 응용서버와 통신하기 위한 소켓 통신모듈로써 TCP로 통신하고 메시지 처리 모듈은 응용서버와 주고 받는 메시지를 처리하는 부분으로 서버에서 수신된 메시지를 분석하여 각 기능 모듈로 분기한다.

3.3 USB 보안 프레임워크 속성 정보

USB 보안 프레임워크의 속성 정보는 USB 보안 프레임워크의 사용자 정보를 이중 사용하는 것을 예방하기 위해서 사용자 인증 전에 보안 토큰내 저장된 이중 사용정보를 인증 서버가 체크한다. 이 때, 인증서버는 사용자의 개인정보가 이중으로 사용되는 것을 체크하기 위해서 (그림 3)과 같은 필드를 USB 장치로부터 전달받아 인증서버의 데이터베이스에 저장되어 있는 정보와 비교 후 정보가 일치할 경우 통신을 지속하고 일치하지 않으면 통신을 중지하도록 한다. 사용자의 정보는 사전에 안정한 경로를 통해 서버에 저장한다고 가정한다.

ID	$\exp_i$	$time$	$Check\ \ Info.$	$Group$

그림 3. 보안 토큰내 저장된 이중사용 유·무 정보
Fig. 3. Double Using Information saved within Security Token

그림 3에서 각 필드의 세부적인 정보는 다음과 같다.

- ID : 보안 토큰에 저장되어 있는 사용자의 신원정보
- $\exp_i$: 인증서버로부터 전달받은 사용자 정보의 현재 유효상태
- $time$: 사용자 정보의 유효시간
- $Check\ Info.$: 사용자의 개인정보 이중 사용 유무정보 (0 or 1)
- $Group$: 사용자 그룹 정보

3.3 USB 보안 프레임워크의 인증 동작과정

USB 보안 프레임워크의 인증과정에서는 USB 디바이스 자체의 특징 및 관리서버에 저장되어 있는 인증 정보에 해당하는 보안 정보를 USB 보안 토큰에 저장한다. 보안 토큰은 일정 시간동안 사용가능하며, USB 모듈들은 USB 보안 토큰을 인증하기 위해서 인증서버에 인증여부를 확인하는 것이 아니라 보안 토큰을 사용해 인증 유·무 정보를 서버를 통해 확인한다.

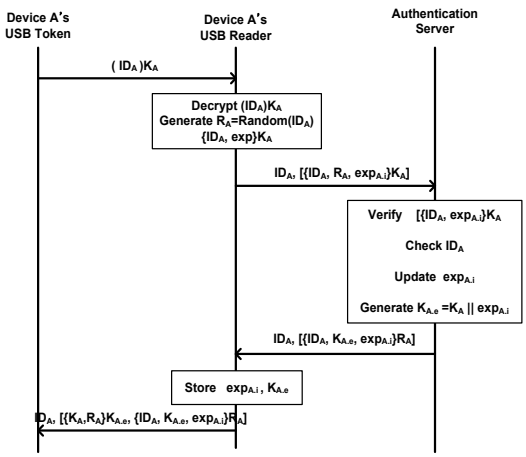

그림 4 USB 인증 과정
Fig 4. USB Authentication Process

(그림 4)는 USB 리더를 통해 USB 보안 토큰을 인식한 후 USB 보안 토큰에 저장되어 있는 인증 정보를 인증서버로 전달하여 사용자의 이중사용 유무를 판단하여 USB를 인증하는 인증과정을 보여주고 있다. (그림 4)의 USB 인증과정에서 보안 토큰을 전달받은 각 USB 디바이스는 인증서버로부터 사전에 인증서버에 등록한 공개키(PU_K)와 개인키(PR_K)를 전달받는다. 전달받은 공개키(PU_K)와 개인키(PR_K)를 계속적으로 사용하지 않고 사용자의 보안 토큰을 인증서버에 등록하는 과정에서 발급받은 유효상태 정보 $\exp_i$ 를 조합하여 유효 공개키($PU_{K.e}$)와 유효 개인키($PR_{K.e}$)를 생성한다. 유효상태 정보 $\exp_i$를 사용하는 경우 보안 토큰의 보안키를 갱신하지 않고 서버에 보안 토큰을 요청할 경우에 보안 토큰내에 저장되어 있는 유효상태 정보 $\exp_i$와 사용자의 개인정보 이중 사용 유무 정보 $Check\ \ Info.$를 체크하여 보안 키의 갱신 유•무를 통해 사용자를 인증할 수 있다.

Ⅳ. 평가

4.1 보안 평가

제안된 USB 보안 프레임워크에서는 사용자의 이중사용을 예방하기 위해서 USB 디바이스는 사전에 인증서버에 등록된 공개키(PU_K)와 개인키(PR_K)를 인증서버에 등록하는 과정에서 발급받은 유효상태 정보 $\exp_i$와 조합하여 유효 공개키($PU_{K.e}$)와 유효 개인키 ($PR_{K.e}$)를 생성하여 8비트 단위로 연산이 이루어지기 때문에 시차를 이용한 Timing 공격을 예방할 수 있다.

USB 보안 토큰과 인증 서버 사이에서 발생가능한 공격 방법 중 재전송 공격을 예방하기 위해서 USB 토큰의 ID를 Random() 함수에 적용하여 랜덤수 R을 사용하여 인증을 수행한다. USB 토큰과 인증서버 사이의 신뢰성을 높이기 위해서 USB 토큰는 인증서버에게 인증정보를 검증받은 후에 USB 보안 토큰과 인증서버 사이에서 유효상태 정보 $\exp_i$에 따라 인증과정이 다르게 수행되기 때문에 repay 공격을 예방할 수 있다. 또한, USB 보안토큰과 인증서버 사이에서 사용하고 있는 파라미터들의 기밀성을 보장하기 위해 제안된 USB 보안 프레임워크에서는 USB 리더의 개인키로 USB 토큰의 정보(ex. ID)를 암호하여 기밀성을 제공한다. 제안된 USB 보안 프레임워크에서는 유효상태 정보 $\exp_i$ 와 서명 기법을 함께 사용하여 USB 환경에서 발생할 수 있는 제3자의 악의적인 redirect 및 DoS공격을 방지할 수 있다.

4.2 성능 평가

4.2.1 실험환경

이 절에서는 USB 장치간 패킷 인증 지연시간과 처리량을 평가하기 위한 도구로 OPNET을 사용하였다. 실험을 위하여 (표 1)의 실험 시나리오를 사용한다. 실험에서 설정된 USB의 수는 200개이며 USB 리더가 USB를 동시에 인식할 수 있는 최대수는 25로 설정한다. USB 토큰은 USB 리더를 통해 인증서버로 데이터 패킷을 전송하고 3600초 동안 실험을 수행한다. USB 토큰의 버퍼 크기는 100패킷의 크기를 가지는 것으로 가정하며, 각 패킷은 패킷 전송동안 패킷 드롭 확률을 0.01로 한다. 이 같은 설정은 현실 모델에 맞는 시뮬레이션을 만들기 위한 설정들이다.

표 1. 실험 환경
Table 1. Experiment Environment

환경 변수	값
USB 수	200
동시 USB 최대 인식수	25
실험시간	3600 s
버퍼 크기	100 packet/s
패킷 드롭 확률	0.01
데이터 패킷 크기	100 bytes
쿼리 패킷 크기	25 bytes
헤더 패킷 크기	25 bytes

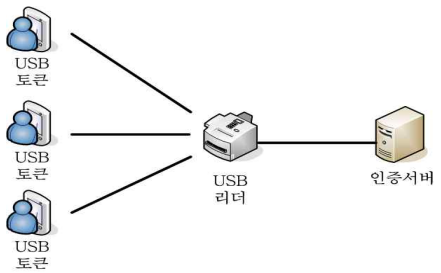

그림 5. 실험 시나리오
Fig 5. Simulated Scenario

제안된 USB 보안 프레임워크의 실험 환경은 (그림 5)와 같다. (그림 5)에서 USB 리더가 USB 토큰을 동시에 인식할 수 있는 최대 수는 50으로 하였으며 시간에 따른 서버의 패킷 인증 지연시간과 인증 처리량을 중심으로 성능 실험을 수행한다.

4.2.2 실험결과

(그림 6)는 USB 인터페이스를 사용하는 단순파일 저장매체(USB driver), 자체 연산 가능한 매체(USB Token)과 제안된 USB 보안 프레임워크를 비교평가하고 있다. (그림 6)는 USB 리더가 USB 토큰을 최대 50개까지 인식 할 수 있도록 설정 한 후 USB 장치 수에 따른 평균 인증 지연시간을 평가하고 있다. 실험 결과 제안기법은 단순파일 저장매체(USB driver)와 자체 연산 가능한 매체(USB Token)보다 각각 9%와 5% 향상된 결과를 보이고 있다. 이 같은 결과는 제안 기법이 USB 토큰의 속성정보에 따라 인증과정을 달리하기 때문에 나타난 결과이다.

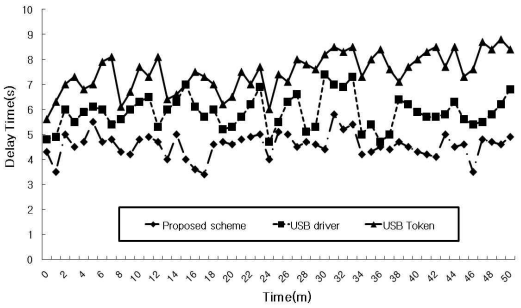

그림 6. 패킷 인증 지연시간
Fig 6. Packet Authentication Delay Time

(그림 7)은 USB 장치 수에 따른 인증서버의 처리량을 나타내고 있다. 단순파일 저장매체(USB driver)와 자체 연산 가능한 매체(USB Token)에서는 USB 장치수가 평균 10, 30, 50 일경우 병목현상으로 인해 인증서버의 처리량이 급격하게 늘어나는 현상이 발생하였으며, 제안된 USB 프레임워크는 사전에 인증서버에 등록된 공개키(PU_K)와 개인키(PR_K)를 인증서버에 등록하는 과정에서 발급받은 유효상태정보 $\exp_i$와 조합하여 유효 공개키($PU_{K.e}$)와 유효 개인키($PR_{K.e}$)를 생성하여 8비트 단위로 연산이 이루어지기 때문에 USB 장치 수 증가에 따른 처리량이 단순파일 저장매체(USB driver)와 자체 연산 가능한 매체(USB Token)보다 처리량이 일정비율로 증가하고 있다.

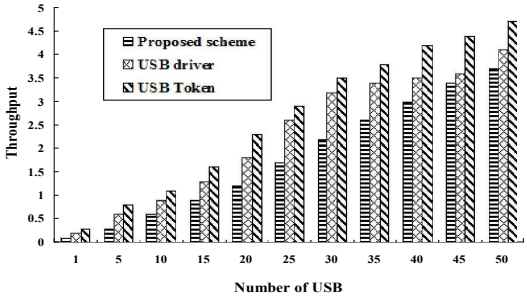

그림 7. USB 수에 따른 처리량
Fig 7. Throughput through USB Number

V. 결론

본 논문에서는 USB 보안 토큰 제품의 이중사용을 예방하기 위해서 USB 보안 토큰 제품이 비밀번호를 설정할 때 사용자에게 입력받은 비밀번호와 속성정보를 이용하여 USB 보안 토큰 제품의 이중사용을 예방하는 보안 프레임워크를 제안하였다. 제안된 USB 보안 프레임워크는 서로 다른 네트워크에서 USB 보안 제품을 사용할 경우 USB 보안 토큰의 사용유·무 및 사용자의 속성 정보를 인증 정보 앞에 4비트를 추가하여 사용자의 인증 과정을 수행하기 때문에 통신 오버헤드 및 서비스 지연이 향상되었다. 실험 결과 단순파일 저장매체(USB driver)와 자체 연산 가능한 매체(USB Token) 보다 제안된 USB 보안 프레임워크가 패킷 인증 지연시간에서 평균 7.6% 향상되었으며 USB 수에 따른 인증서버의 처리량에서도 평균 9.8% 향상된 결과를 얻을 수 있었다. 향후 연구에서는 제안된 메커니즘을 여러 종류의 USB 환경에 적용할 수 있는 하이브리드 통합 보안 프레임워크를 연구할 계획이다.

참고문헌

[1] A. Ghosh, D. R. Wolter, J. G. Andrews and R. Chen, "Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential", IEEE Communications Magazines, vol. 43, issue 2, pp. 129~136. Feb. 2005.

[2] TTAS.KO-06.0065R1, "Air and Network Interface Specifications for 2.3GHz band Portable Internet Service -MAC", TTA Standard, 2004.

[3] IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems",

2006.
[4] IETF RFC 4285, "Authentication Protocol for Mobile IPv6", 2006.
[5] WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures", 2007.
[6] D. I. Kim, S. H. Lee, Y. J. Kim, "Mobility Management in WiBro/Mobile WiMAX", The Korean Institute of Information Scientists and Engineers, vol. 25, No. 04, pp. 5~14. 2007. 04.
[7] T. Janevski, "Traffic analysis and design of wireless IP networks", Artech House, pp. 186~190, 2003.
[8] A. Mishra, M. Shin and W. Arbaugh, "pro-active Key Distribution using neighbor Graphs", IEEE Wireless Communication, vol. 11, Feb 2004."
[9] M. Kassb, A. Belghith, J. M. Bonnin and S. Sassi, "Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks", In Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling, pp. 46-53, 2005.
[10] D. Sweeney, "WiMax Operator Manual: building 802.16 Wireless Networks", Apress, 2005.
[11] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.

저 자 소 개

정 윤 수

2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
2008년 2월 : 충북대학교 대학원 전자계산학 박사
2009년 8월 ~ 현재 : 한남대학교 산업기술연구소 전임연구원
관심분야: 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
Email : bukmunro@gmail.com

이 상 호

1989년 2월 : 숭실대학교 대학원 컴퓨터네트워크 공학박사
1981년 6월 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수
관심분야: Protocol Engineering, Network Security, Network Management, Network Architecture
Email : shlee@chungbuk.ac.kr