MPC860을 이용한 PC카드 보안토큰 장치구동기 및 API 설계/구현

김기홍*, 박종욱*, 윤장홍*

*국가보안기술연구소

An Implementation Device Driver and API for PC Card Cryptographic Token Using MPC860

Ki-hong Kim*, Jong-wook Park*, Jang-hong Yoon*

*National Security Research Institute

요 약

PC카드 형태로 개발되어 사용되는 보안토큰은 다양한 보안서비스를 바탕으로 차세대 정보보호 기술의 핵심기술로 떠오르고 있다. PC카드 보안토큰 휴대용 컴퓨터 운용을 위한 메모리 카드 표준 인터페이스를 수용하여 다양한 암호알고리즘 수행이 가능하고, 사용자의 요구조건을 비교적 쉽게 수용하고, 아울러 다양한 응용분야에 사용되는 등의 장점을 가지고 있다. 본 논문에서는 Motorola PowerPC 기반의 MPC860 마이크로 프로세서가 장착된 제어보드를 이용하여 PC카드 보안토큰에 대한 PCMCIA(Personal Computer Memory Card International Association) 카드 장치구동기 및 API(Application Program Interface)를 설계/구현하여 각각의 기능시험을 통해 그 기능들을 검증하였다.

I. 서론

최근 정보통신 기술의 급속한 발전과 인터넷 확산은 다양한 형태의 업무환경 및 생활환경을 바꾸어 놓았다. 그러나, 이러한 변화와 병행하여 정보의 도용, 변조, 획득, 불법 접근 등의 다양한 위협요소들에 노출될 가능성은 더욱 더 커지고 있다. 따라서, 이러한 위험요소에 대한 대책으로 정보보호 서비스의 필요성이 대두되었다[1-3].

일반적으로 보안토큰은 주로 카드 형태, 즉 PCMCIA 카드와 스마트카드로 개발되어 사용되고 있다. 스마트 카드는 메모리와 CPU를 탑재하여 자기 카드에 비해 기억용량이 크고 CPU가 내장되어 있어 데이터 처리능력을 가지고 있다. 또한, 암호 처리, 접속대상 인증, 기억 데이터의 관리 등의 보안 기능이 뛰어나 은행 카드, 신분증명 카드, 유료 방송수신 카드 등으로 사용되는 장점을 가지고 있으나, 외부 인터페이스를 위한 전송속도가 매우 낮아 고속시스템에 접속하여 사용하기에는 한계가 있다[2]. 이에 반해 PCMCIA 카드는 스마트 카드보다 강력한 암호관련 연산처리를 수행하며 다양한 응용분야에 사용된다. 또한, 초고속 시스템에 직접 접속할 수 있어 고속의 보안서비스를 제공할 수 있다[3]. 본 논문에서는 이러한 PC카드 보안토큰이 제공하는 다양한 보안서비스의 이용을 위해 Motorola PowerPC 기반의 MPC860 마이크로 프로세서가 장착된 제어보드를 이용하여 PCMCIA 카드 장치구동기 및 Cryptoki API를 설계/구현하여 각각의 기능시험을 통해 그 기능들을 검증하고자 하였다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 PC카드 보안토큰의 일반적인 구조 및 기능을 설명하고, 3장에서는 MPC860 마이크로 프로세서의 기본적인 기능과 MPC860내의 PCMCIA 호스트 어댑터 모듈을 설명하며, 4장에서는 설계된 장치구동기 및 API를 설명하며, 5장에서는 설계된 장치구동기 및 API에 대한 각각의 기능시험을 통해 그 기능들의 검증결과를 제시하고, 6장에서 결론을 맺는다.

II. PC카드 보안토큰 구조 및 기능

본 논문에서 사용한 보안토큰은 PCMCIA 인터페이스 표준을 채택하고 있으며, PCMCIA 인터페이스 표준을 지원하는 데스크탑 PC, 휴대용 PC, 그리고 PCMCIA 인터페이스를 지원하는 마이크로프로서가 탑재된 통신장비 및 정보보호장비 등에 접속하여 사용할 수 있다.

그림 1은 일반적인 PC카드 보안토큰의 구조를 보여주고 있다[4]. 그림에서 보는 것처럼, 고성능 프로세서, 프로그램 저장을 위한 램, 부트롬, 보안토큰의 부팅과 진단 기능을 담당하는 진단 프로그램, 암호칩 등으로 구성되어 있다. 이러한 하드웨어 구조를 바탕으로 PC카드 보안토큰은 다양한 고속의 보안서비스 기능을 제공하게 된다.

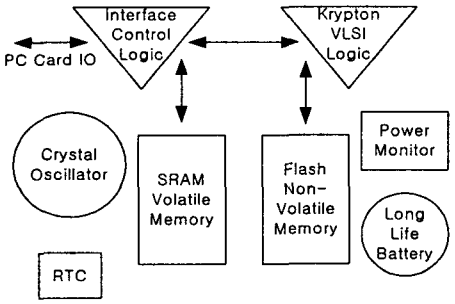

그림 1: PC카드 보안토큰 구조.

III. MPC860 개요 및 HBA 모듈

1. MPC860 마이크로 프로세서

MPC860은 Motorola의 MC68360 QUICC(QUad Integrated Communication Controller) PowerPC 기반의 변형된 형태로, CPU는 MMU(Memory Management Unit)와 명령/데이터 캐쉬 등을 통합한 32비트의 PowerPC 구현이다. 또한, PowerPC RISC(Reduced Instruction Set Computer) 프로세서, 메모리 컨트롤러, 인터럽트 컨트롤러, 통신용 RISC 프로세서를 내장하고 있는 SOC(System On Chip) 타입의 임베디드 프로세서이다[5,6].

그림 2는 MPC860의 전체적인 구성도를 보여주고 있다.

2. HBA(Host Bus Adapter) 모듈

일반적으로 PCMCIA 인터페이스 환경을 하드웨어적 관점에서 보면, 그림 3과 같다[7]. 호스트 시스템은 PC카드 보안토큰과의 정합을 위해 HBA 모듈을 필요로 한다. 따라서, 호스트 시스템인 MPC860이 PC카드 보안토큰과 정합되기 위해서는 HBA를 구현하여야 한다. 호스트는 MPC860 내부 제어레지스터 영역 내에 메모리-맵 되어 있는 PCMCIA 인터페이스 관련 레지스터들(PBR, POR, etc)을 세팅함으로서 PC카드 보안토큰과의 정합을 위한 HBA를 구현할 수 있는 것이다.

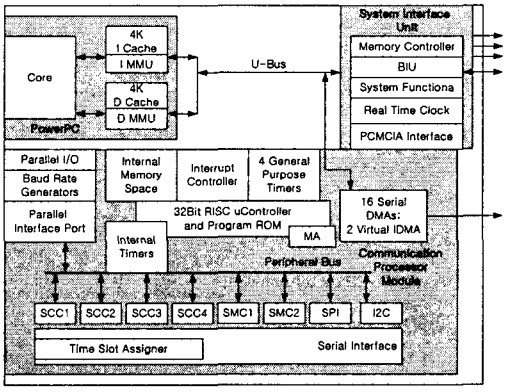

그림 2: MPC860 구성도.

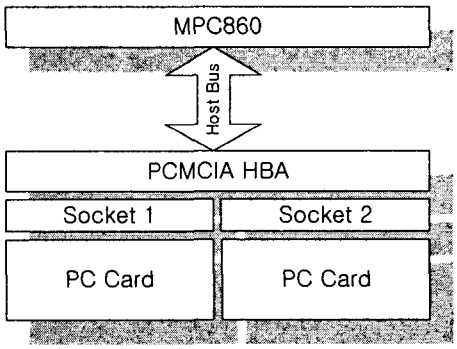

그림 3: PCMCIA 인터페이스 환경.

IV. 장치구동기 및 API 설계/구현

1. PC카드 보안토큰 장치구동기

장치구동기는 응용프로그램을 통하여 하드웨어를 제어하는 프로그램으로 PC카드 보안토큰의 검출/제거를 감시하며, PC카드가 가지고 있는 메모리를 응용프로그램에서 액세스할 수 있도록 한다[8]. 본 논문에서는 MPC860이 장착된 제어보드, Diab Data 4.0b 컴파일러, BDM(Background Debugger Module), GNU nmake 등을 사용하여 PC카드 보안토큰 장치구동기를 개발하였다.

MPC860내의 내부 제어레지스터들 중 PCMCIA 인터페이스를 제어하는 레지스터들은 표 1과 같으

며, 이들 각각의 레지스터들을 세팅함으로써, 또한 PCMCIA 인터페이스 할당을 위한 MPC860 인터럽트 소스를 구현함으로써 장치구동기를 구현하게 된다.

표 1: PCMCIA 인터페이스 레지스터.

PIPR	PCMCIA Interface Input Pins Register
PSCR	PCMCIA Interface Status Changed Register
PER	PCMCIA Interface Enable Register
PGCRA/B	PCMCIA Interface General Control Register A/B
PBR[0-7]	PCMCIA Base Register[0-7]
POR[0-7]	PCMCIA Option Register[0-7]

MPC860은 그림 4와 같이 SIU와 CPM에 각각 인터럽트 컨트롤러가 내장되어 있다. CPM 인터럽트 컨트롤러는 29개의 인터럽트 소스를 받아서 SIU 인터럽트 컨트롤러의 레벨 중에 하나로 연결되고, SIU 인터럽트 컨트롤러는 PowerPC IREQ에 연결된다. 본 논문에서는 모니터링 및 디버깅을 위한 RS-232C 인터럽트 소스는 레벨 4에, 보안토큰을 위한 PCMCIA 인터럽트 소스는 레벨 5로 할당하였으며, 0x0000000h에 exception vector table의 시작위치를 할당하였다.

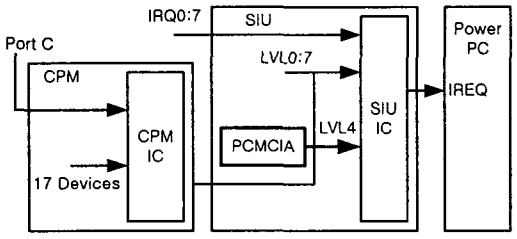

그림 4: MPC860 인터럽트 구성도.

장치구동기는 크게 3가지 부분 - 보안토큰 검출/제거, 전원 센싱/공급·차단, 리셋 - 으로 나눌 수가 있다. 호스트는 이를 이용하여 보안토큰의 다양한 보안서비스 이용을 위한 보안토큰 초기화를 수행할 수 있으며, 초기화 과정은 다음과 같다.

① PIPR 값을 읽어온다.(PCM_PIPR)

② PIPR 값을 바탕으로 보안토큰 검출/제거 및 전원 센싱/공급·차단을 수행한다.(CD_PIPR, VS_PIPR, PCM_POWER)

③ 일정 시간지연을 준다.(PCM_DELAY)

④ 리셋.(PCM_RESET)

⑤ 리셋 여부를 체크한다.(CHK_RESET)

⑥ 보안토큰의 속성 메모리 영역과 공통 메모리 영역 설정을 위해 PBR, POR을 세팅한다.(MEMORY_SET)

⑦ 보안서비스를 시작한다.(APPLICATION)

그림 5는 보안토큰 초기화와 관련된 보안토큰 검출, 전원 공급, 그리고 신호 공급 등의 과정을 보여주고 있다[7].

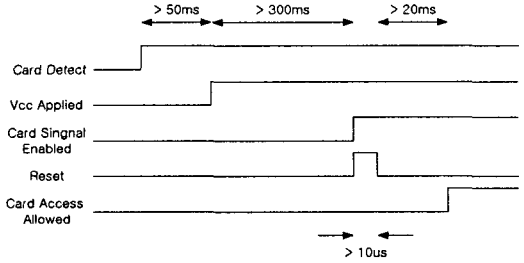

그림 5: 보안토큰 검출 및 전원/신호 공급.

2. PC카드 보안토큰 API

현재 개발되어 사용되는 정보보호 서비스 API는 IETF의 GSS-API/IDUP-GSS-API, ㅌ/OPEN의 GCS-API, Microsoft의 CryptoAPI, RSA의 Cryptoki 등이 있으며, 본 논문에서는 RSA의 Cryptoki[9]를 채택하였다. 이러한 API는 암/복호화 기능 및 다양한 암호체계, 디지털 서명, 해쉬 함수, 난수 발생기 등을 제공하도록 설계되었으며 표 2는 API에서 제공하는 각각의 세부기능들을 보여준다.

표 2: Cryptoki API 함수.

기능	설명
범용 함수	보안토큰의 사용/종료시 사용
슬롯 및 토큰관리 함수	보안토큰의 슬롯 및 토큰정보 획득
세션관리 함수	세션 획득 및 종료
객체관리 함수	객체 생성 및 제거
암/복호 함수	암/복호 수행
HASH/MAC 함수	해쉬 및 MAC 함수 수행
이중목적관리 함수	암/복호 및 해쉬 동시 수행
키관리 함수	비밀키 및 대칭키 생성
난수발생 함수	난수 생성

RSA의 PKCS #11 v2.10을 만족하도록 설계된 API는 응용프로그램에서 호출된 명령을 장치구동기를 통해 보안토큰에 전달하거나 장치구동기로부터 전달된 응답을 응용프로그램으로 전달한다. 따라서, 호스트는 보안토큰의 세부사항에 대한 지식 없이도 API에 접근하여 보안토큰을 사용할 수가 있다. 설계된 정보보호 서비스 API는 데이터 암/복호화를 포함하여 다양한 보안서비스를 제공하며, 응용프로그램에 대한 AppID와 SessionID를 관리한다. 또한, 각각의 함수에 해당하는 명령코드와 아규먼트 등을 보안토큰이 인식할 수 있는 명령으로 변환하여 호스트에서 보안토큰으로 전달하는 기능 등을 담당한다.

V. 시험 및 검토

본 논문에서는 아래에 주어진 구현환경과 제어보드 및 소프트웨어 환경을 이용하여 PC카드 보안토큰 장치구동기 및 API를 설계/구현하고, 아울러 시험용 프로그램을 작성하여 각각의 기능을 시험하였다.

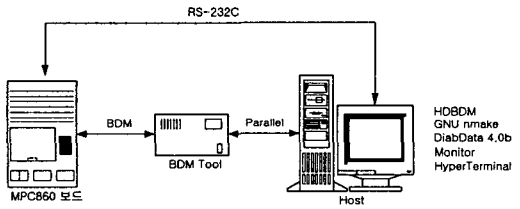

그림 6: 구현환경.

BDM 툴인 Haedong BDM은 MPC860이 장착된 제어보드와 BDM 컨넥터로 연결되고, 호스트와는 parallel 포트로 연결된다. 제어보드와 호스트와는 RS-232C 컨넥터로 연결되어 캐릭터의 입/출력을 수행하고, 모니터 및 시험용 프로그램을 이용하여 장치구동기를 이용한 보안토큰 초기화와 API 기능들을 시험하고 검증하였다.

표 3: MPC860 제어보드 및 소프트웨어 환경.

제어보드	MPC860, Flash Memory, SDRAM, etc
BDM 툴	Haedong BDM
BDM 소프트웨어	HDBDM
컴파일러	Diab Data 4.0b
Make	GNU nmake
모니터 프로그램	Hyper Terminal

응용프로그램은 명령을 API에 전달하고 API에서는 전달된 명령을 분석하여 장치구동기에 명령을 전달한다. 이를 바탕으로 장치구동기는 보안토큰에 명령을 전달하고 보안토큰이 이를 분석/처리하여 장치구동기로 응답을 전달하면, API를 통해 응용프로그램에게 응답을 전달한다. 응용프로그램은 그 응답결과를 모니터를 통해 호스트에게 보여주는 것이다.

표 4는 본 논문에서 수행된 장치구동기와 API의 기능시험 항목을 보여주고 있으며, 이들 각각의 기능들을 시험을 통해 검증하였다.

표 4: 기능시험 항목.

항목	설명
검출/제거 시험	보안토큰이 PCMCIA 인터페이스로의 검출/제거 동작상태 확인
전원공급 시험	보안토큰의 전원 센싱을 바탕으로 일정 전원을 공급하고 동작상태 확인
전원차단 시험	전원을 차단하고 동작상태 확인
CIS 데이터 획득 시험	속성 메모리 영역에 저장되어 있는 CIS 데이터 획득
PCMCIA 인터럽트 소스 시험	레벨 5로 할당된 인터럽트 서비스 루틴을 수행하고 동작상태 확인
범용, 슬롯/토큰, 세션관리 함수 시험	보안토큰에서 전달된 응답데이터 값들을 사전에 정해진 데이터 값들과 비교
암/복호화 관련 시험	특정 암호알고리즘을 이용하여 암/복호화를 수행하고 응답데이터 값들을 사전에 정해진 데이터 값들과 비교
무한루프 수행 시험	무한루프를 수행하여 위의 항목들을 시험

VI. 결론

본 논문에서는 Motorola PowerPC 기반의 MPC860 마이크로 프로세서를 이용하여 PC카드 보안토큰이 제공하는 다양한 보안서비스의 이용을 위한 PCMCIA 카드 장치구동기 및 Cryptoki API를 설계/구현하여 각각의 기능시험을 통해 그 기능들을 검증하였다. 모니터 및 시험용 프로그램을 이용하여 보안토큰 검출/제거, 전원 공급/차단,

Cryptoki API 함수 등의 기능들을 시험하고 올바른 동작상태 및 응답데이터 값들이 사전에 정해진 응답데이터와 동일한 값들을 가짐을 확인하였다. 앞으로, 본 논문에서 구현된 장치구동기 및 API는 효율적인 보안서비스 시스템 설계를 가능하도록 할 것이며, 또한 다양한 RTOS(Real Time OS)를 지원할 수 있도록 장치구동기 및 API를 개발하고자 한다.

참고문헌

[1] 박상현, 김영수, 양상운, "PC 카드형 보안모듈 API 및 장치 구동기 설계 및 구현", WISC 2001, pp. 649-658, 2001년 9월.
[2] 박영수, 김호원, 정교일, "차세대 IC 카드 기술 개발", SIC 2001, pp. 399-413, 2001년 7월.
[3] home.nownuri.net/~migrator/tech/index13.html
[4] www.rainbow.com/mykoweb/fpcblok.htm
[5] Motorola, *MPC860 PwerOUICC™ User's Manual*, 1998.
[6] Motorola, *PowerPC Microporcessor Family: The Programming Environments For 32-Bit Microprocessors*, 1997.
[7] Michael T. Mori, *The PCMCIA Developer's Guide Second Edition*, Sycard Technology, 1995.
[8] Walter Oney, *Programming the Microsoft for Windows Driver Model*, Microsoft Press, 2000.
[9] RSA, PKCS #11 v.2.10:Cryptographic Token Interface Standard, 1999.