USB를 이용하는 보안 토큰 시스템의 구현

김 영 진, 반 성 범, 정 용 화
한국전자통신연구원 생체인식기술연구팀
{youngjk, sbpan, ywchung}@etri.re.kr

An Implementation of a Security Token System using USB

Young-Jin Kim, Sung-Bum Pan, Yong-Wha Chung
Biometrics Technology Research Team, ETRI

Abstract

The match-on-token is a system which executes the user-authentication on the system using the user's biometric information. Nowadays, due to increase of request of the secure user-authentication on various parts, it comes to more use.

In this paper, the match-on-token system under development by ETRI is described. The system consists of a host and an emulator board. USB is employed as the communication channel between them. First, the booting code of the emulator board was programmed and tested in order that USB programs and the finger-print matching program can be executed correctly. Then, host programs cooperating with the board was designed, implemented and tested. Finally, future research including optimization of applications on the match-on-token will be mentioned.

1. 서론

근래에 전자상거래, 전자 화폐 등의 폭넓은 사용에 따라 개인 정보의 해킹에 대한 위협도 커지고 있어 이의 안전한 관리 및 안전한 사용자 인증이 요구되고 있는 실정이다. 현재 주로 사용되고 있는 개인 인증 방법인 패스워드나 개인 번호의 사용은 해킹 또는 관리 부주의에 따른 노출이 쉬워서, 보다 안전한 사용자 인증 방법이 필요하다. 보안 토큰 시스템은 지문, 얼굴, 음성 등의 생체 정보를 개인 식별을 위한 인증 자료로서 이용하는데, match-on-token을 구축하는데 이용된다. Match-on-token은 기준이 되는 사용자 생체 정보를 미리 토큰 내에 가지고 있고, 인증이 필요할 때 외부에서 생체 정보를 받아 들여 토큰 내에서 정합(matching)을 수행한다. 이로써, 호스트를 포함한 토큰 외부에서 일어 날 수 있는 사용자 정보에 대한 해킹을 방지하게 된다. 또한, match-on-token은 스마트 카드를 이용한 match-on-card로 연계되어 발전하고 있다.

본 논문에서는 한국전자통신연구원에서 개발하고 있는 match-on-token 형태의 보안 토큰 시스템에 대해 기술한다. USB 통신을 이용하는 보안 토큰 시스템을 에뮬레이터 보드 형태로 구현하고 지문 생체 정보를 탑재하여 지문 정합 프로그램을 탑재하여 수행 및 시험한다. 에뮬레이터 보드는 ARM CPU를 core로 하는 마이크로프로세서를 사용하고 있는데, 보드의 구동을 위한 부팅 코드와 USB를 이용하기 위한 보드 및 호스트 프로그램을 구현 및 시험하였으며 지문 정합 프로그램을 탑재하여 수행하고 그 내용을 살펴보았다. 또한, 추후 과제를 위한 내용과 내년도 목표인 match-on-card으로의 전이를 위해 필요한 내용들을 간단히 언급하였다.

2. 보안 토큰 시스템 설계

일반적인 보안 토큰 시스템은 서론에서 언급한 바와 같이 생체 정보를 이용하여 시스템 내에서 사용자 인증을 수행하므로 인증 과정상의 안전성을 보장하게 된다. 즉, match-on-token상에서 생체 정보 정합을 수행한다. 본 논문에서의 보안 토큰 시스템에서 사용되는 생체 정보는 지문으로 한정하도록 한다.

지문을 이용한 보안 토큰 시스템은 사용자 등록(enrollment) 과정과 사용자 인증 과정(authentication)으로 이루어 진다. 사용자 인증 과정은 지문 특징점의 정합을 포함한다. 이 과정을 도식으로 보인 것이 그림 1이다.[1]

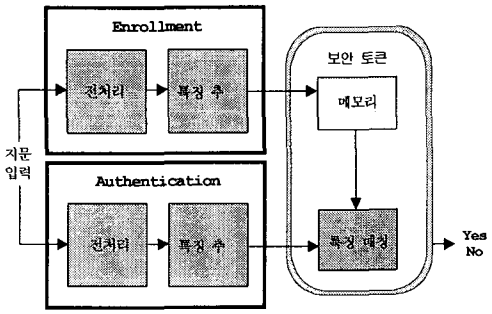

그림 3 일반적인 match-on-token 시스템[1]

등록 및 인증 과정에서 입력된 지문 영상을 이용한 특징점 정보 추출과정까지는 호스트에서 수행한다. 등록 및 인증 지문 특징점 정보는 USB 통신 채널을 통해 보안 토큰에 저장한 후에는 외부로 전달되지 않고 개인 기기 내부에서 정합 과정까지 수행하여 인증 결과만을 외부로 출력하도록 한다. 보안 토큰의 메모리 크기 및 CPU 연산 성능에 따라 보안 토큰의 지문 정합 수행 성능이 달라지므로 이에 대한 고려가 반드시 필요하다. 본 장에서는, 보안 토큰 에뮬레이터 보드에서의 H/W 사양 및 S/W 수행 환경 설계, 호스트 프로그램의 설계, USB 통신 및 지문 정합 프로그램의 수행에 대해 기술한다.

2.1 보안 토큰 에뮬레이터 보드

보안 토큰은 에뮬레이터 보드의 형태로 구현되는데, ARM7TDMI를 core로 하는 상용 프로세서를 CPU로 사용한다[4]. 메모리 뱅크를 이용하여 메모리 맵 설정 및 초기화를 하며 강력한 디버깅을 위해 JTAG을 이용한 AXD 디버거를 사용하도록 하고 상위 레벨의 간단한 디버깅 또는 모니터링을 위해 직렬 통신을 사용한다. 또한, 보드와 호스트와의 통신을 위해서 USB 통신을 지원하도록 한다. 이러한 내용을 포함한 보안 토큰 보드의 H/W 구조를 나타내면 그림 2와 같다.

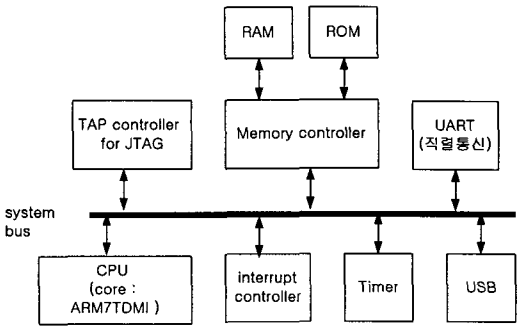

그림 4 보안 토큰 에뮬레이터 보드 구조

보안 토큰 보드에서의 수행 S/W는 H/W와 직접 인터페이스하는 장치 구동 루틴을 포함하고 이용하는 부팅 코드와 응용 프로그램으로 나뉜다. 장치 구동 루틴은 메모리 설정 관련 레지스터에 대한 동작, 직렬 통신 장치 및 USB 장치에 대한 초기화 및 인터럽트 처리 함수 등이 포함된다. 이를 수용하는 부팅 코드 및 응용 프로그램의 수행 절차는 다음과 같다.

①메모리(SDRAM, DRAM 등) 설정 및 초기화
②관리자 모드 설정
③인터럽트 제어 register 초기화 및 설정
④전역 코드 영역 및 데이터 영역 초기화
⑤각 모드별 스택포인터 설정
⑥예외 벡터 테이블 설정
⑦사용자 모드 설정 및 스택포인터 설정
⑧응용 프로그램(지문정합 프로그램)의 메인함수 호출

2.2 호스트 프로그램

보안 토큰 보드는 호스트에서 동작하는 클라이언트(client) 프로그램에서 넘겨주는 데이터에 대해 지문 정합을 수행한다. 이 데이터는 기준이 되는 지문 특징점 정보와 인증을 위해 입력을 받는 지문 특징점 정보이다. 이 지문 특징점 정보들은 호스트에 연결된 지문 스캐너에 연결되어 영상 이미지로부터 특징점 추출을 담당하는 프로그램으로부터 얻어지게 된다.

호스트측에서의 USB 통신을 위한 프로그램은 USB 허브를 제어하고 USB 1.1 spec.에 맞도록 통신 내용을 제어하는 드라이버와 상위 클라이언트 프로그램으로 나뉜다. USB 드라이버는 Microsoft에 의해 제공된 Windows Driver Development Kit(DDK)를 이용, 수정하여 재작성할 수 있다.[2]

3. 보안 토큰 시스템 구현 및 시험

3.1 보안 토큰 시스템 구현

현재 개발중인 보안 토큰 시스템은, ARM core를 내장한 마이크로프로세서 에뮬레이터 보드상에서 ARM Developer Suite(ADS) 1.1로 부팅 코드 및 시스템 소프트웨어를 구현하고 있으며 호스트상에서는 Windows 98 운영체제를 기반으로 MS Visual C++ 6.0으로 클라이언트 환경을 구축하였다.

에뮬레이터 보드는 ARM7TDMI를 core로 하며 부팅 롬으로 flash ROM 256K bytes, 프로그램 수행 공간으로 SDRAM 16M bytes를 가지며 디버깅 및 모니터링을 위한 직렬 통신 포트, 지문 추출 정보의 송수신과 이를 이용해 사용자 인증을 하기 위한 USB controller 및 hub를 가지고 있다. 부팅 코드는 SDRAM의 인식 설정 및 초기화를 시작으로 관리자 모드 및 인터럽트 모드에서의 stack point 설정, 인터럽트 제어 register 초기화와 예외 벡터 테이블의 RAM 설치 등을 포함한다. 그림 3은 구현하여 사용하고 있는 보안 토큰 에뮬레이터 보드의 모습을 보이고 있다.

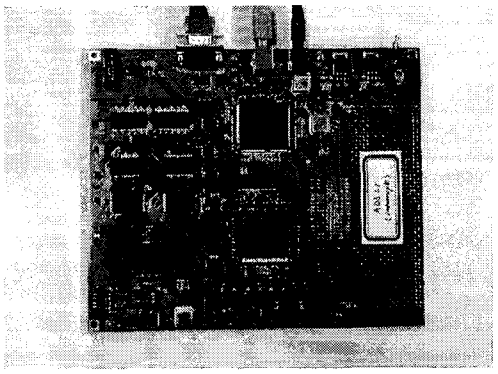

그림 5 보안 토큰 에뮬레이터 보드

USB 소프트웨어는 1.1 spec.에 따라 호스트의 드라이버와 bus enumeration을 수행한 뒤에 인터럽트에 의해 송수신을 하도록 구현되었다. USB 통신을 위한 호스트 프로그램은 보드의 USB 디바이스 드라이버에서 지원하는 Bulk 및 interrupt transfer 타입 통신을 모두 지원하도록 구현되어 있다. 그림 4는 호스트와 보안 토큰에서의 USB 구성 계층간의 통신 모델을 나타 낸 것이며, 최상위에 존재하는 계층, 즉 클라이언트 프로그램과 보안 토큰상의 USB 함수가 구현되어 사용되고 있다. 그림 5는 지문 정합 프로그램과의 USB 통신을 고려한 지문 정보를 이용하는 보안 토큰 시스템의 구성도를 보인 것이다. 이 구성도를 기반으로 실제 보안 토큰 시스템의 수행 절차를 간략히 작성한 내용이 그림 6에 나타나 있다.

한편, 보드에서 사용되는 지문 정합 프로그램은 한국전자통신연구원의 생체인식기술연구팀에서 개발한 피라미드 기법을 적용하여 제한된 수행 메모리를 사용하여 지문 정합을 수행하도록 하고 있다.[1] 피라미드 알고리즘은 기존 방식에 비해 지문 특징점 정합시에 비교 단위를 단계적으로 조정함으로써 수행 메모리의 크기를 줄이고 있다.

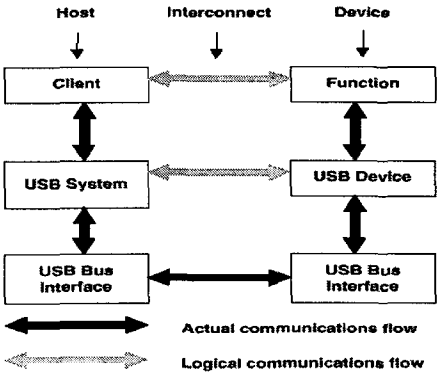

그림 6 USB 통신 모델 [3]

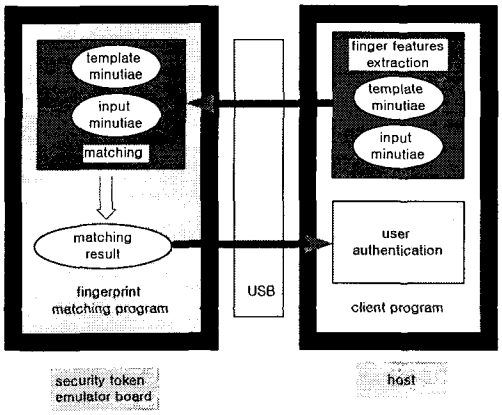

그림 5 보안 토큰 시스템 구성도(지문 정보 이용)

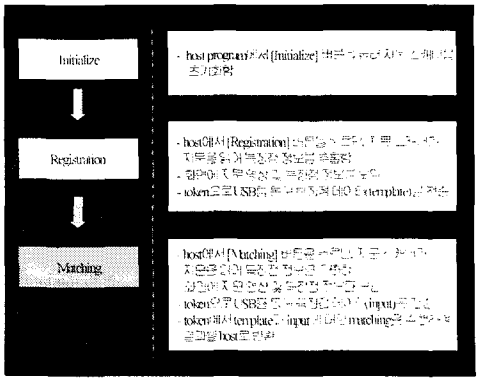

그림 8 보안 토큰 시스템 수행 절차

3.2 보안 토큰 시스템 시험

보안 토큰 시스템의 시험은 그림 6의 수행 절차에 따라 그림 3의 보드와 호스트 PC를 연결하여 시험하였다. 현재 지문 스캐너 및 특징점 추출 프로그램은 구현된 내용에 포함되어 있지 않으므로 Initialize 단계에 따른 동작은 아무런 수행을 하지 않도록 되어 있다. 따라서, Registration 단계에서는 이미 만들어져 있는 특정한 지문 특징점 정보를 가지고 있다가 추출된 정보로 가정하여 수행에 이용하게 된다. 이때, 기준이 되는 지문 정보는 20개의 특징점으로 구성되는데, 하나의 특징점은 x변위, y변위, 각 변위, 방향 및 특징점 종류로 구성된다. 또, 입력 특징점 정보는 같은 사용자의 특징점이나, 기준 정보에 대해 값들이 상이한 16개의 특징점으로 구성되어 있다. 그림 7은 직렬 통신을 통해 보안 토큰에서의 프로그램 수행을 제어할 수 있는 터미널 화면을 보이고 있으며, 그림 8은 Matching 단계에서, 호스트 프로그램이 앞에서 기술한 지문 특징점 정보 2쌍의 정보를 보드로 USB를 통해 송신하고 정합 결과를 다시 수신하여 그 결과를 간단히 보이는 모습을 나타내고 있다.

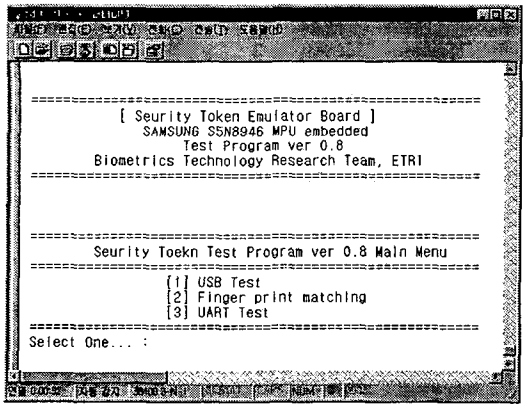

그림 9 보안 토큰과의 직렬 통신을 위한 터미널 화면

4. 결론

보안 토큰 시스템은 안전한 사용자 인증의 요구를 만족시키기 위해 사용되고 있는데, 사용자의 생체 정보를 보안 토큰 상에서 인증함으로써 정보 유출이나 해킹에 대해 안전하다.

본 논문에서는 보안 토큰 시스템을 설계 및 구축하는 내용과 기 추출된 기준 지문 특징점 정보에 대해 입력 특징점 정보를 USB를 통해 호스트로부터 보안 토큰 에뮬레이터 보드에 전송받아 정합 프로그램을 수행하고 시험하는 내용을 기술하였다. 이를 위해서 먼

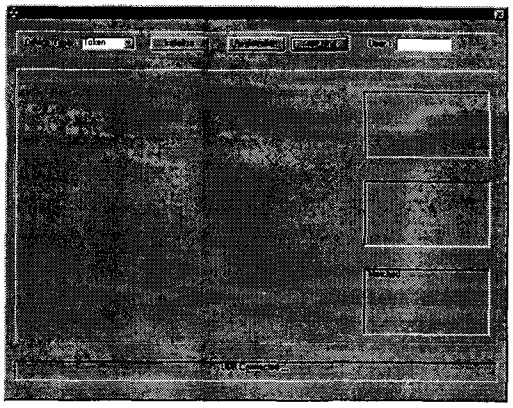

그림 10 호스트 프로그램

저, 보안 토큰 에뮬레이터 보드의 H/W와 S/W를 구현하고 I/O인 USB을 사용하는 보드 프로그램과 호스트 프로그램을 구현하였다. 이후에 지문 정합 프로그램을 보안 토큰에 응용 프로그램으로 탑재하여 사용자 지문의 특징점 데이터에 대해 올바른 정합 수행 여부를 살펴보았다.

추후 과제로서는, 시스템 관점에서의 응용 프로그램 최적화 즉, 정합 프로그램의 수행 시간 및 수행 메모리 크기에 대한 최적화에 대한 일들이 요구된다. 수행 속도와 사용 메모리 크기는 서로 병치되는 일이므로 이에 대한 선택적 최적화 연구가 필요하다. 현재는, 이를 위해서 수행 시간 측정을 위한 timer 구동 루틴과 메모리(힙 및 스택) 측정 루틴을 작성하고 시험하고 있다. 나아가서, 스마트 카드를 이용한 match-on-card 시스템은 자원의 제약이 더욱 심하므로 보드에서의 메모리 제한에 대한 최적화된 지문 정합 프로그램의 작성 및 수행이 요구된다.

참고문헌

[1] 반성범 외, "사용자 인증을 위한 Match-on-Card 시스템에 관한 연구", 제2회 생체인식기술 워크샵, 2002. 1.

[2] 장승석, Bulk transfer를 위한 USB host (Windows 98 PC) 프로그램 구성, 한국전자통신연구원 기술문서(TM-1700-1999-095), 1999.10.

[3] Universal Serial Bus Specification 1.1, Sep. 23. 1998.

[4] S5N8946 ADSL/Cable Modem Microcontroller User's Manual, Rev. 1.1, SAMSUNG, 2001.