스마트카드를 이용한 사용자 인증 및 관리

박종원° 이긍해
한국항공대학교 컴퓨터 공학과
{pecker96°, khlee}@mail.hangkong.ac.kr

User Authentication and Management Using Smart Card

Jongwon Park° Keunghae Lee
Department of Computer Engineering, Hankuk Aviation University

요 약

최근 컴퓨터 및 다양한 디바이스들을 이용하여 인터넷 서비스를 제공받는 사용자가 많아지고 있다. 이러한 인터넷 서비스를 제공받기 위해서 사용자는 서비스 제공사이트에서 요구하는 개인정보를 입력하거나 인증절차를 거치게 되는 경우가 많이 생긴다. 기존 인증방법의 경우 고정된 패스워드로, Keystroke 해킹 등 각종 해킹으로 개인 정보 유출 가능성이 높다. 본 논문은 스마트카드를 이용하여 이러한 문제점을 해결하는 것을 목표로 한다. 스마트카드를 이용하여 다양한 디바이스에 연결 할 때 기존 패스워드 방식이 아닌 Q/A 방식으로 개인만이 알 수 있는 몇 개의 임의의 질문에 답변 하는 방식으로 개인 정보를 원하는 곳에 안전하게 사용할 수 있는 사용자 인증과 관리방법을 제안한다. 그리고 제안된 사용자 인증 및 관리 방법에 대해 설명한다.

1. 서 론

최근 컴퓨터 및 다양한 디바이스들을 이용하여 인터넷 서비스를 제공받는 사용자가 많아지고 있다. 인터넷을 이용하는 사용자들은 휴대폰, PDA, 휴대 컴퓨터 등과 같이 다양한 디바이스들을 언제 어디서나 이용하여 인터넷에 접근할 수 있는 유비쿼터스 환경으로 발전되었다.[1] 이러한 인터넷 서비스를 제공받기 위해서는 사용자는 서비스 사이트에서 요청하는 개인정보를 입력해야 한다. 또한 사용자들은 개인 디바이스뿐만 아니라, 공용 디바이스를 이용하여 서비스 제공사이트에서 요청하는 개인정보를 입력하거나 인증절차를 거치게 되는 경우가 많다.[4] 이 경우 다른 프로그램에 의해서 개인 정보가 유출될 수 있는 가능성이 높아진다. 따라서 개인 정보의 유출을 방지하기위해 새로운 인증방법이 필요하며, 자동으로 관리해주는 사용자 편의를 높일 수 있는 방법이 요구되고 있다.

본 논문은 스마트카드를 이용하여 이러한 문제점을 해결하는 것을 목표로 한다. 스마트카드를 이용하여 PC를 포함한 다양한 디바이스에서 사용가능하고, 언제 어디서나 전자상거래, 전자 금융 거래에 있어 안전하게 개인정보를 원하는 곳에 사용할 수 있는 사용자 인증과 관리 방법을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 본 시스템 개발에 필요한 관련기술에 대해 설명하고, 3장에서는 스마트카드를 이용하여 개인정보를 사용할 때 필요한 요구사항들에 대해서 설명한다. 4장에서는 본 논문에서 제안하는 Smart Card를 이용한 사용자의 인증방법과 전체적인 구조 및 구성내용에 대해 설명하고 이 구조를 적용한 시나리오를 5장에서 서술한다. 그리고 6장에서 결론을 맺는다.

2. 관련기술

2.1. 자바카드

자바카드는 스마트카드의 운영체제에 자바 바이트코드 인터프리터를 탑재하고, 카드에 적합하게 변환된 자바 클래스 파일을 다운로드 할 수 있는 스마트카드이다. 각각의 스마트카드들은 카드마다 다른 종류의 하드웨어와 이러한 하드웨어를 운영하는 운영체제인 COS(Card Operating System)를 가지게 된다.[3]
또한 COS위에 SUN사가 개발한 자바 카드 가상 머신(Java Card Virtual Machine)을 탑재한 형태의 스마트 플랫폼으로 다중 응용 프로그램 탑재가 가능하고 post-issuance 형태로 응용 프로그램 다운로딩이 가능한 개방형 플랫폼이다.

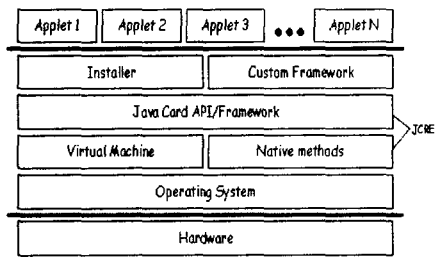

그림1. 자바카드 내부구조

자바카드는 중앙처리장치, ROM, EEPROM, RAM과 같은

메모리가 존재하는 하드웨어 계층 위에 카드 운영체제, 자바카드 상에 다양한 응용 프로그램이 존재할 수 있도록 지원해주는 자바 카드 가상 머신이 탑재되며, 자바카드 가상머신 위로 자바 카드 API, 자바 카드 애플릿(Applet)이 순서대로 탑재된다. 자바 카드 내부구조는 그림 1과 같이 볼 수 있다.

자바카드 가상 머신은 2개의 분리된 구조로 구성되는데, 이는 제한된 메모리 자원을 갖는 카드의 특성을 고려하여 수행시간이 오래 걸리고, 메모리 자원을 많이 사용하는 부분은 단말기 상에서 처리하도록 한 것이다. 자바 카드 가상 머신은 그림2와 같다.

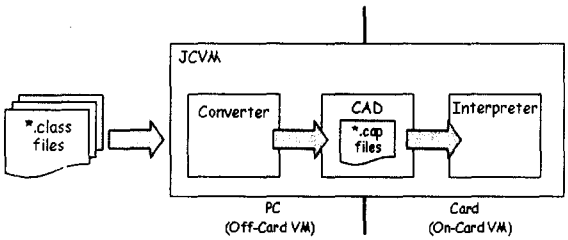

그림2. 자바 카드 가상 기계 머신

PC 및 단말기에 위치하는 Off-card VM은 클래스 파일 로딩, 링킹, 변환, 바이트 코드 최적화, 클래스 파일 검사, 객체 및 배열 초기화 등의 기능을 담당하며, 카드 상에 위치하는 On-card VM은 바이트코드실행, 객체 생성 및 메모리 제어 등의 기능을 담당하는 인터프리터를 의미한다. Off-card VM을 대표하는 컨버터는 패키지 단위로 변환작업을 수행하고, 입력으로 패키지(클래스집합)와 export 파일을 받아들여 CAP(Converted Applet)파일과 새로운 export파일을 출력한다. CAP 파일은 자바카드 상에 응용 프로그램을 post-issuance 형태로 다운로드 할 경우에 사용되는 파일형태로 실행코드 및 클래스 정보, 링킹 정보등을 담고 있으며, export 파일은 클래스 파일 링킹 및 검사를 위한 링킹 정보(public API)를 포함하고 있다. 자바 가상머신과 마찬가지로 자바 카드 가상머신 역시 다양한 카드 운영체제에 탑재되어 수행될 수 있는 특징을 갖고 있기 때문에, 자바 응용 프로그램은 플랫폼과 무관하게 동작한다.

2.2. 암호 알고리즘 및 암호 모듈기술

일반적으로 스마트카드는 사용자에게 강화된 보안성 및 안정성을 제공해주기 위하여 플랫폼에 암호 알고리즘이나 암호 알고리즘의 수행시간을 가속화해주는 하드웨어 가속기를 구현하여 사용자의 데이터를 보호하거나 사용자 및 단말기 인증을 수행하는데 이용한다.[8]

자바카드의 경우 자바카드 API 중 암호 API 확장 패키지를 이용하여 암호 알고리즘과 관련된 키 관리, 키 생성, 암호 알고리즘 함수 호출 등을 수행하며, 알고리즘의 수행시간을 개선하기 위해 native methods 기능을 사용한다. Native methods는 자바 응용 프로그램에서 자바 카드 API를 통해서 접근할 수 없는 하위 플랫폼 기능을 사용하고자 할 경우, 자바 언어로 구현되지 않은 라이브러리를 사용하는 경우, 마지막으로 암호 알고리즘 프로그램의 수행속도를 향상시키고자 할 경우에 이용하는 방법이다.

3. 요구사항

인터넷을 통한 전자상거래, 전자 금융 거래 등은 사용자에게 편리성을 제공해주지만 개인정보가 쉽게 노출될 수 있는 문제점을 가지고 있다. 특히 공동으로 사용하는 디바이스의 경우 Keystroke와 같은 각종 해킹에 노출되어 있다. 이처럼 인터넷을 통한 금융거래 및 개인 정보 등이 언제 어디서나 편리하고 안전하게 이루어지기 위해서는 다음과 같은 특징을 만족시켜야한다.

- 개인정보보호 (Privacy)
- 실시간 지원 (Real-time supports)
- 호환성 (Interoperability)
- 편리성 (Convenience)
- 확장성 (Extensibility)
- 신뢰성 (Reliability)
- 휴대성 (Portability)

위의 조건을 만족시키기 위해 본 논문에서는 스마트카드를 이용한 사용자 인증 및 관리 방법에 대하여 제안한다.

4. 스마트카드를 이용한 사용자 인증 및 관리

사용자는 개인정보를 스마트카드에 저장하여 키보드를 통해 일어나는 Keystroke 해킹 및 각종 해킹으로부터 벗어나 안전하게 사용 및 관리하고자 한다.

이를 위해 본 논문에서는 개인정보가 저장되어 있는 스마트카드와 각 디바이스 간에 인증 및 관리 방법을 제안한다. 첫 번째로 스마트카드에서 각 디바이스에 할 때의 인증방법에 대해 설명하고, 두 번째로 개인정보 인증 및 관리 방법의 전체적인 구조에 대해 설명한다.

4.1 사용자 인증 및 관리방법

스마트카드에서 각 디바이스를 연결할 때의 인증방법은 기존의 Password와 같은 숫자와 문자를 조합한 방식이 아닌 Q/A방식의 인증방법을 이용한다. 즉, 개인만이 알 수 있는 몇 개의 임의의 질문을 던져 답을 받는 형식을 가진다.

예를 들면 당신이 존경하는 인물은?, 당신이 가장 아끼는 것은? 와 같은 형식으로 개인만이 알 수 있는 질문을 사용자가 저장하여 인증 하는 방법이다.

개인이 직접 인증 형식을 정하기 때문에 개인은 아무 문제없이 인증 받을 수 있으며, 기존 패스워드처럼 한번의 인증 절차가 아닌 몇 개의 임의의 질문이기 때문에 개인만이 사용 가능한 인증 방법이다. 또한 스마트카드를 분실했을 때에 기존의 숫자와 문자를 조합한 방식처럼 고정된 패스워드가 아니기 때문에 개인 중요 정보가 유

출될 위험성이 줄어들게 된다.
관리 방법은 질문에 상관없이 개인이 특별히 정한 답으로 개인정보를 수정 및 추가 그리고 삭제 할 수 있다.

4.2 사용자 인증 및 관리방법의 전체적인 구조

스마트카드를 이용하여 각 디바이스를 접속하기 위한 개인정보 인증 및 관리방법의 전체적인 구조는 그림 3과 같다.

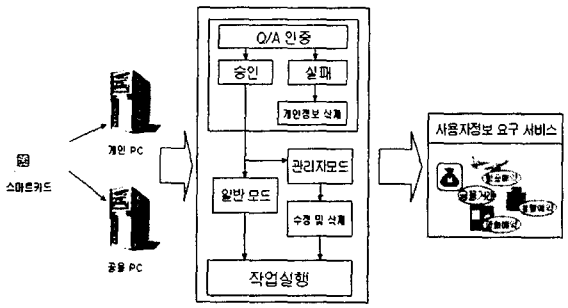

그림3. 개인정보 인증 및 관리방법의 전체적인 구조

전체적인 구조는 스마트카드가 디바이스에 삽입되었을 때부터 사용자정보를 요구하는 서비스에 개인정보를 사용 할 때의 과정을 보여준다.

스마트카드 인증은 Q/A인증방법으로 사용자가 정한 몇 개의 임의의 질문을 보내 답을 받는 형식으로 3번 이상 틀렸을 경우, 자동으로 스마트카드 내에 개인정보가 삭제된다. 또한 일반모드와 관리자모드로 구성이 되어 일반모드에서는 개인장치를 포함한 다른 디바이스에서 사용할 때 사용되며, 관리자모드는 개인정보를 수정하거나 삭제할 때 사용된다.

5. 적용 시나리오

K기업의 메일 서버 관리자인 보희는 휴가 기간에 스키장에 갔다. 스키를 타고 있던 그녀는 직장 동료로부터 메일서버에 이상이 생겼다는 전화를 받았다. 급하게 숙소로 돌아온 그녀는 숙소로 돌아와 스마트카드를 챙겨 숙소 근처 PC방으로 향했다. PC방에서 그녀는 자신의 스마트카드를 PC에 삽입하고 인증절차를 거친 후에 스마트카드에 저장된 주소로 접속하여 자신이 관리하는 메일서버에 접속했다. 메일 서버가 관리자ID와 비밀번호를 요구하자 스마트카드 내에 저장된 ID와 비밀번호를 안전하게 관리자 페이지에 삽입하였고 그녀는 Keystroke 해킹에 안전한 상태로 자신의 서버에 접속을 해 이상여부를 확인하고 복귀 시킬 수 있었다.

6. 결론

본 논문에서는 다양한 디바이스에서 스마트카드를 이용한 사용자 인증과 관리방법에 대하여 제안하였다.
사용자가 스마트카드를 이용하여 다양한 디바이스에서 안전하게 개인 정보를 원하는 곳에 사용 가능하고 인증 및 관리하는 방법에 대하여 설명하였고, 이를 통해 다양한 디바이스에 스마트카드를 삽입함으로써 이루어지는 인증방법으로 분실시를 대비하여 고정된 패스워드 방식에서 벗어나 Q/A방식의 몇 개의 임의의 질문을 통해 개인만이 사용가능한 방법을 제안 하였다. 또한 개인정보 유출의 위험성을 줄이고 안전하게 원하는 서비스를 제공하고자 하였다.

향후 여기에서 제안된 스마트카드를 이용한 개인정보 인증 및 관리방법을 이용하여 유비쿼터스 본래 정의처럼 언제 어디서나 사용가능하고 다양한 디바이스에 개인정보를 안전하게 이용함으로써 원하는 곳에 응용 가능 할 것이다.

참고문헌

[1] Mark Weiser, "The Computer for the Twenty-First Century:", Scientific American, pp94-101, September 1991.
[2] http://www.tta.or.kr
[3] Timothy M.Jurgensen, Scott B.Guthery, "SmartCards The Developer's Toolkit", Prentice Hall PTR, 2002
[4] Ronald Ashri, S.Atkinson, D.Ayers, M.Haglind, B.Ray, Rob.M, N.Nashi, R.Taylor, C.Wiggers, "Professional Java Mobile Programming" Wrox, 2001
[5] 류지현, 이긍해, "Stream Cipher 알고리즘을 이용한 온라인상의 개인정보관리 시스템", 한국정보과학회 추계 학술발표대회 제출, 2003.
[6] Keung Hae Lee, Oh Wha Park, "Research on TSpace", IBM Almaden Research Center, 2000
[7] Alexander Joseph Huber, Josef Franz Huber, 이근호, 이상근, 박승창, 한호현, 이기혁, 배석희 "유비쿼터스 모바일 컴퓨팅", 진한도서, 2001
[8] JavaCard 2.2 API Specification, Sun Microsystems, Inc., Early Access, 2001