Journal of Korea Multimedia Society Vol. 14, No. 2, February 2011(pp. 249-257)

스마트카드를 이용한 위조방지 인증 시스템 설계 및 구현

김 은[†], 이윤석[††], 정민수[†††]

요 약

다양한 상품에 대한 시장의 보호를 위해 기존 기술적 인증 기술은 ID, 홀로그램, 그리고 RFID를 사용하는 등 점차 발달하고 있다. 하지만 이와 같은 방식은 인증 매체와 인증 정보가 노출되어 있어 이에 대한 복제가 쉬워, 위조품을 원천적으로 방지할 수 없다. 본 연구에서는 이와 같은 문제를 해결하기 위하여, 스마트 카드 내에 명품의 인증정보, 사용자 정보, 그리고 매장의 정보를 안전하게 저장 및 관리할 수 있도록 JCVM File System을 설계 하였으며, 스마트 카드의 프로세서를 활용하여 정보를 노출시키지 않고 안전한 인증이 가능한 인증 프로토콜을 설계 및 구현하였다. 이를 통해 위조품의 발생을 원천적으로 차단시킬 수 있으며, 스마트 카드가 부착이 가능한 어떠한 상품에도 인증의 용도로 활용할 수 있다.

Design and Implementation of an Authentication System for Anti-Forgery using the Smart Card

Eun Kim[†], Yun-Seok Lee[††], Min-Soo Jung[†††]

ABSTRACT

To protect the market for various products, existing authentication techniques using ID, hologram and RFID have been gradually developed. However, these methods can be easily exposed the authentication information, and also these exposed information easily copy. Thus, production of the counterfeit goods can not completely prevent. In this paper, to solve these problems, we designed JCVM file system for saving and managing the authentication information, user's information and a sales agency information into the smart card. And we designed and implemented an authentication protocol that can authenticate to avoiding exposure using processor of the smart card. Through this, this proposed scheme can prevent occurrences of the counterfeit goods. And also, can be used for authentication as any product that can attach the smart card.

Key words: Anti-Forgery(위조방지), Smart Card(스마트카드), Authentication(인증)

1. 서 론

오늘날 건전한 시장의 안전을 해치는 위해 요소 중 가장 큰 것은 바로 위조품이라 할 수 있다[1]. 위조품의 생산 및 확대는 작게는 한 개인의 구매 상품과 관련된 것일 수 있지만, 크게는 시장 거래의 중요한 요소 중 하나인 신용을 무너뜨리는 요소가 되기도 하고, 때로는 국가간의 무역 분쟁의 소지가 되기도

※ 교신저자(Corresponding Author) : 정민수, 주소 : 경상남도 창원시 마산합포구 월영동 449번지 경남대학교 1공학관 8층 자바OS 실습실(631-701), 전화 : 010)6574-7633, FAX : 055)248-2554, E-mail : msjung@kyungnam.ac.kr
접수일 : 2010년 12월 13일, 수정일 : 2011년 1월 14일
완료일 : 2011년 1월 20일
[†] 준회원, 경남대학교 컴퓨터공학과
(E-mail : silver0891@naver.com)
[†††] 준회원, 경남대학교 컴퓨터공학과
(E-mail : lysis2jt@naver.com)
[†††] 종신회원, 경남대학교 컴퓨터공학과
※ 본 연구는 2010년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2010-0017069)

한다. 그러므로 과거부터 다양한 방식의 위조품을 차단 시키기 위한 법적, 제도적 장치와 기술적 장치가 요구되어 왔다[2]. 오늘날의 위조품을 방지하기 위한 기술로서는 상품에 ID를 부착하는 방식, 제조사와 상품의 고유한 특징 및 마크를 삽입한 홀로그램 방식, 그리고 상품의 정보가 저장되어 있는 RF tag를 활용한 RFID 방식등이 있다[3]. 하지만 ID 방식의 경우에는 인증 정보가 노출 되어 있어 해당하는 ID 정보를 단순한 복사를 통해서도 위조품이 발생하게 되는 단점이 있으며, 홀로그램 방식의 경우에는 ID 방식에 비해 정보를 은닉할 수 있으나, 홀로그램 생산 장비를 구매하여 대량으로 위조품을 만들어 내는 것을 방지할 수 는 없다[4]. 그리고 RFID 방식의 경우에는 고성능의 암호 알고리즘이 탑재되지 않아, 인증 정보가 인증단계에서 노출되기가 쉬우며, 이에 따라 이역시도 저가의 RFID tag를 생산할 수 있는 기기만 갖추면 대량으로 위조품을 생산할 수 있다. 이와 같이 기존의 방식에서는 대량으로 생산되는 위조품을 원천적으로 차단할 수 없으며, 이에 따라 정당하게 구매한 제품의 대량 생산 및 유통으로 인해 소모되는 사회적 비용은 상당히 크다고 할 수 있다.

본 논문에서는 이러한 위조품의 발생을 원천적으로 차단하기 위하여, 반지 등과 같은 엑세서리 형태로도 탑재가 가능하고, 기본적으로는 카드와 같은 형태로 구성되어 있는 스마트 카드 내에 인증 정보와 사용자 정보 그리고 매장 정보를 안전하게 저장 및 관리 할 수 있도록 JCVM File System을 설계 및 구현하였으며, 고강도 암호 알고리즘인 RSA 암호 알고리즘을 사용하여 인증 정보를 노출시키지 않고 안전하게 인증센터(Authentication Center)와 통신을 수행하는 인증 프로토콜을 설계 및 구현하였다. 이에 따라 위조품의 생산을 원천적으로 방지할 수 있으며, 다양한 형태의 스마트 카드가 존재하므로 스마트 카드의 모양 변경에 따라 다양한 상품에 탑재하여 안전하게 정당한 제품의 인증을 수행할 수 있다.

본 논문의 2장에서는 기존의 위조품 방지 대책을 나열하고 해당하는 방식의 장 단점을 분석하는 관련 연구를 그리고 3장에서는 제안하는 시스템의 설계를 4장에서는 구현 및 테스트, 5장에서는 기존 방지 대책과의 비교 분석을 제시하고, 마지막 6장에서는 결론을 도출한다.

2. 관련연구

2.1 ID 기반 인증방식

ID 기반 인증 방식의 경우에는 해당하는 상품에 ID를 기록하고 해당 ID가 정당한 상품인지를 인식하는 방식으로, 간단하게는 바코드와 같은 형태의 구조를 가지고 있다. 이와 같은 방식의 경우에는 인증을 위한 정보가 숫자와 문자의 조합 또는, 바코드와 같이 특정 선과 기호의 조합으로 이루어진다. 장점으로는 간단한 인증과, 인증 매체를 생산하는 단가가 아주 저렴하다는 장점이 있으나, 인증 정보가 스캔 후 인쇄, 복사기를 통한 정보의 재 출력 등이 가능하고, 이에 다라 대량으로 손쉽게 복사가 가능하다는 단점이 있어 주로 아주 저가의 상품에 대한 위조 방지책으로 활용되고 있다.

2.2 홀로그램 기반 인증 방식

홀로그램 기반 인증 방식의 경우에는 해당하는 상품에 사용자의 시점의 변화에 따라 서로 다른 상이 나타나는 방식으로 다층화된 필름을 겹쳐 생산하는 방식으로 ID 기반 인증 방식에 비해 복제가 어려운 장점이 있다. 하지만, 이 역시도 다층화된 필름을 인쇄하여 생산가능한 장비를 구매하여 위조품에 대한 대량 생산이 이루어지는 등, 사실상 위조품을 방지하는 것에는 한계가 있으며, 상품의 정당한 홀로그램이 아니라, 위조한 조잡한 홀로그램이라 할지라도, 사용자가 정당한 홀로그램인지를 알 수가 없으므로, 인증에 있어서 인증 주체의 인식률이 높지 않다는 단점이 있다[5].

2.3 Smart tag 기반 인증 방식

Smart tag의 경우에는 기존 바코드에서의 2차원의 정보에 따른 인증이 아닌, 3차원 정보를 통해서 다양한 형태의 정보가 기록이 가능하다는 장점이 있어, 현재 URI 와 같은 정보들을 기록하고 있는 추세이다. 이에 따라 해당하는 tag 정보를 상품에 부착하여 인증하는 용도로 활용이 가능하나, 사실상 이 Smart tag 역시도 바코드와 같이 스캔, 복사 등을 통한 대량 생산이 가능하기 때문에 위조 방지책으로 활용하는 것에는 한계가 있다.

2.4 RFID 기반 인증 방식

RFID 기반 인증 방식의 경우에는 RF tag에 상품에 대한 정보를 기록하여 이 기록된 정보 tag를 상품에 부착, 리더기로 해당하는 상품이 정당한지를 인증하는 방식이다. 이 때 인증 정보의 안전성은 RFID의 성능에 따라 크게 달라진다. RFID는 크게 수동형과 능동형으로 구분할 수 있는데, 수동형의 경우에는 자기 자신이 전원을 가지고 있지 않는 형태의 태그이고 능동형 태그의 경우에는 자신이 전원을 가지고 있어 전파식별의 거리가 매우 길다. 이러한 RFID의 경우에는 단순히 숫자와 문자로 조합된 ID 정보만 저장되어 있어 리더로부터 해당하는 동작 주파수를 수신하면 ID 정보를 아무런 암호화나 인증 절차 없이 송신하는 방식으로 이방식의 경우에는 인증 정보가 손쉽게 노출되어 해당하는 인증 정보인 ID를 수신하여 다른 RF tag에 이 정보를 이식하여 위조품을 정상적인 상품으로 인증 가능하도록 하는 방식이 있다[6,7]. 그리고 이를 개선하여 간단한 암호 알고리즘이 탑재되어 운용되는 것의 경우에는 리더로부터 동작 정보를 수신하여 해당하는 ID 정보를 암호화 하여 리더로 송신, 리더는 이에 대한 정보를 복호화 하여 해당하는 ID를 검증하는 방식이다. 이 방식의 경우에는 인증의 키가 tag 당 할당되는 것이 아니라 리더가 가지고 있어야 하므로, 키가 노출될 경우에는 해당하는 모든 tag의 정보들이 다 노출 될 수 있으며, 재연공격을 방지하기 위해서는 매 세션마다 다른 값을 송신하여야 하는데, 이때 난수의 발생에 따른 시간적 지연과, 난수 크기에 따른 보안적 취약성이 발생할 수 도 있다. 그리고 tag 방식으로 인하여 해당 tag의 손상에 약하다는 단점도 있다.

2.5 Smart Card 구조

본 논문에서 인증정보를 저장 및 탑재 관리할 스마트 카드의 구조는 그림 1에서 보는 것 과 같다. 스마트 카드는 기본적으로 CPU와 ROM, RAM 등의 프로세서와 저장 공간이 존재하여 다양한 형태의 어플리케이션이 탑재 가능하고, Crypto Processor를 전용으로 탑재한 것도 있어 공개키 기반 방식과 같은 고강도 암호화 알고리즘 역시도 고속으로 처리 할 수 있도록 설계 되어 있다.

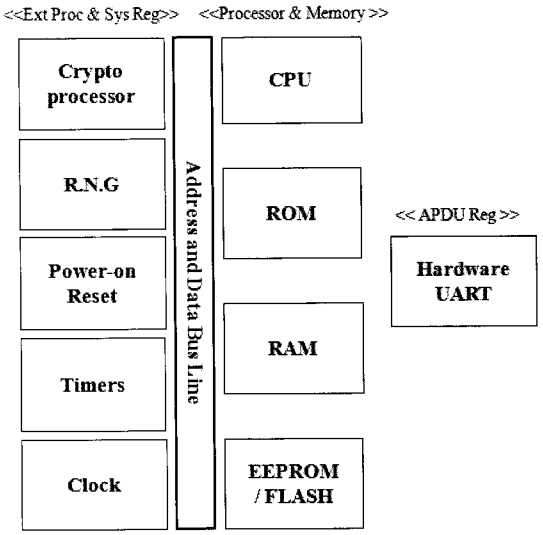

그림 1. Smart Card의 구조

본 논문에서는 이러한 스마트 카드 구조에 자바카드 가상기계인 JCVM을 탑재하여 운용할 것이다. 이는 인증 기법 및 인증 정보가 변하더라도 손쉽게 후발급의 형태로 탑재 운용할 수 있도록 하기 위해서이다[8-13].

3. 제안 시스템의 설계

위조품을 원천적으로 방지하기 위한 제안 시스템은 그림 2에서 보는 것과 같다. 먼저 스마트 카드가 탑재된 상품이 존재하고 이 상품은 인증 정보의 기록 또는 인증에 사용되는 호스트와 통신을 수행한다. 그리고 이 호스트는 상품의 인증 센터(AuC)와 안전한 통신을 수행하여 인증을 완료한다.

이때 스마트 카드내에 자바카드 가상기계를 탑재하고 해당하는 자바카드 가상기계에 인증을 위한 전용 파일 시스템을 구축하여야 한다. 이는 단순히 인증 정보만을 저장 및 관리하는 것 보다, 스마트 카드의 메모리와 프로세서를 적극적으로 활용하여 사용

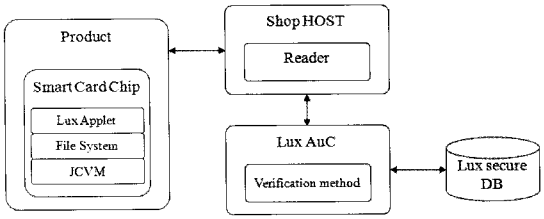

그림 2. 제안 시스템의 시스템 구성도

자의 편의성을 향상시킬 수 있는 정보들을 함께 저장 유지할 수 있도록 하기 위함이다. 그리고 또한 제안하는 시스템에서는 통신상의 노출정보가 단순한 인증 정보뿐만 아니라, 안전한 통신이 가능할 수 있도록 상호인증 프로토콜을 제안하여 인증을 수행할 수 있도록 설계 하였다.

3.1 제안 시스템의 인증 JCVM File System

본 논문에서 제안하는 인증 정보는 스마트 카드에 자바가상기계를 탑재한 자바카드에 저장 된다. 이 자바카드에 정보를 저장하는 방식은 Applet에 직접 기록하는 방법과 File System을 통한 저장 및 관리 방법이 있다. 본 논문에서는 상품의 재 판매, 상품의 보증기간의 변경 등에 효과적으로 대처할 수 있도록 자바카드 가상기계에 인증 전용 파일 구조를 설계 하였다. 이 파일 구조는 그림 3과 같다.

자바카드 가상기계의 파일 시스템은 기본적으로 ISO7816-4 스마트 카드 표준 파일 구조에 따라 설계 되었다. 해당하는 파일은 MF라는 최 상위 파일을 기준으로 하여, 인증 전용 파일 구조를 설계 하였다. 인증 정보는 크게 3가지로 구분하였다.

- *Authentication Information = {LuxName, LuxID, Manufacture Name, Manufacture Address}*
- *User Information = {User Name, User ID}*
- *Shop Information = {Shop ID, Date of Purchase, Date of Warrant}*

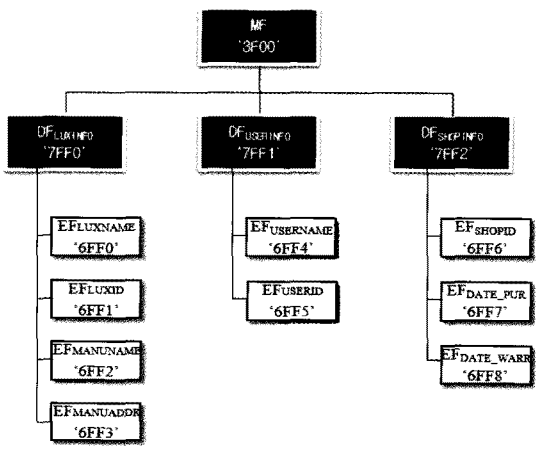

그림 3. 제안 시스템의 JCVM File Structure

이와 같은 정보를 안전하게 저장할 수 있다. 그리고 해당하는 파일에 대한 외부 접근을 차단하기 위하여 각각의 파일들은 Access Condition을 가지고 있는데, 본 논문에서는 기본적인 인증이 애플릿의 PIN 검증을 통한 인증을 수행하여야만 해당하는 파일에 접근 할 수 있도록 설계하여, 인증 애플릿을 제외한 프로그램이 해당 파일에 접근하는 것을 방지하여 파일 자체에 대한 안전성을 확보하였다.

3.2 제안 시스템의 인증 Protocol

본 논문에서 제안하는 인증 프로토콜은 크게 3부분으로 구성된다. 먼저 상품이 제작되어 스마트 카드가 탑재된 상태에서 사용자에 의해 구매가 되기 전 상품이 정당한 상품인지를 초기 인증하는 단계, 구매가 되어 구매된 상품에 대한 다양한 정보를 저장하는 저장 단계, 그리고 최종적으로 상품이 정당한 것인지를 인증하는 인증 단계이다. 각각의 단계에서는 인증정보를 노출시키기 않아야 하며, 호스트에 해당하는 인증정보가 남아 있지 않아야 하는 필수 조건이 따른다. 이를 만족하기 위하여 다음과 같이 설계 하였다.

3.2.1 초기 인증 단계

초기 인증단계는 스마트 카드가 탑재된 상품이 사용자에게 판매되기 전 즉 사용자의 정보가 스마트 카드에 기록되기 전에 판매처에서 해당하는 상품이 위조품이 아님을 사용자에게 정보를 제공하는 단계로 다음과 같은 인증 단계를 거친다.

Step 1 : Reader의 정보요청에 따라 상품은 자신의 난수 Ni를 생성.

그리고 Lux Applet의 PIN 검증 이후 LuxName과 LuxID를 획득.

AuC의 공개키로 LSC=Ekpub(Ni||LuxName||LuxID)를 수행

LSC를 Reader로 송신.

Step 2 : Reader는 자신의 난수 Nj 생성.

자신의 ID인 ShopID를 AuC의 공개키로 SDATA=Ekpub(Nj||ShopID) 수행.

LSC와 SDATA를 AuC로 송신.

Step 3 : AuC는 Dkpri(LSC), Dkpri(SDATA) 수행, Ni,Nj,LuxName,LuxID,ShopID 획득

Secure DB내의 LuxName과 LuxID 확인

RSDATA=((ShopID⊕Nj)⊕Result) 수행, RSDATA Reader로 송신

Step 4 : Reader는 ShopID⊕Nj를 통해 Result 획득. 결과를 사용자에게 확인.

3.2.2 정보 저장 단계

정보를 저장하는 단계에서는 사용자 정보, 판매점 정보를 저장하는 단계로 초기 인증을 거친 뒤, 판매가 이루어지는 시점에서 이루어진다. 이는 상품이 다른 사람에게 재 판매 되더라도 동일한 절차에 의해 정보가 저장 될 수 있도록 설계 되어야 한다. 이에 대한 인증 절차는 다음과 같다.

Step 1 : Reader의 정보요청에 따라 LSC 생성. LSC Reader로 송신

Step 2 : Reader는 자신의 난수 Nj 생성.

사용자로부터 입력받은 USERINFO={User Name, UserID}와, SHOPINFO={ShopID,DATE_PUR,DATE_WARR}를 AuC의 공개키로 SUDATA=Ekpub(Nj||USERINFO||SHOPINFO}생성, LSC, SUDATA를 AuC로 송신

Step 3: AuC는 Dkpri(LSC)와 Dkpri (SUDATA)를 통해 Secure DB에 등록

RSDATA 생성. Reader로 결과 송신

Step 4: Reader는 Result 획득 확인 후 USERINFO, SHOPINFO 스마트 카드에 송신

Step 5 : 스마트 카드는 해당 정보를 File System에 저장.

3.2.3 인증 단계

인증 단계의 경우에는 상품에 인증 정보가 모두 저장되어 있고, 해당하는 상품이 정당한 것인지를 어느 때든 매장 또는 리더가 부착된 호스트 상에서 인증이 가능한 단계이다. 이때 인증 정보는 호스트 상에 남아 있지 않아야 한다. 이에 대한 인증 절차는 다음과 같다.

Step 1 : Reader로 부터의 인증 요청 수신.

해당 파일의 정보 획득, 난수 Ni 생성.

AuC의 공개키로 LUSDATA=Ekpub(Ni||LuxID||UserID||ShopID) 수행.

Reader로 LUSDATA 송신.

Step 2 : Reader는 자신의 난수 Nj 생성

SDATA 생성.

AuC로 LUSDATA와 SDATA 송신.

Step 3 : AuC는 Dkpri(LUSDATA)와 Dkpri (SDATA)를 수행 정보획득.

LUSDATA를 통해 추출된 정보와 Secure DB내의 정보와 비교, RSDATA생성. Reader에 송신

Step 4 : Reader는 Result 획득. 사용자에게 결과 확인.

4. 구현 및 테스트

본 논문에서는 앞서 설계한 시스템에 따라 데스크탑에 위조품인지를 판별하는 인증 센터인 AuC와 리더기가 부착된 호스트를 구성하였고 각각의 통신은 루프백 주소인 127.0.0.1로 통신을 수행하였다. 그리고 스마트 카드에 자바카드 가상기계와 파일구조 그리고 인증 애플릿의 개발 및 탑재는 S3FJ9SK Probe 보드와 AIJI A1000 Emulator를 사용하였으며 정확한 동작의 테스트를 위하여 상품의 ID와 RSA 1024 bit의 공개키 및 개인키를 생산하여 고정된 키 값으로 테스트 할 수 있도록 구현하였다.

4.1 구현

구현은 크게 3부분으로 구성되어 진다. 하나는 JCVM의 파일시스템을 운용하는 인증 애플릿이고, 하나는 리더가 부착된 호스트 그리고 마지막으로 인증정보를 검증하는 인증 센터로 구분된다. 이중 스마트 카드 부분의 인증 흐름도는 그림 4와 같다.

애플릿, 호스트 그리고 인증센터에서는 설계에 따른 3가지 인증 프로토콜 방식에 따라 서로 상이한 통신이 가능하도록 구현하였다.

4.2 테스트

상품에 해당하는 고정된 ID를 생산된 난수와 연접하여 인증 센터의 공개키로 암호화 하여 송신하고 해당하는 정보를 검증하는 것으로 테스트 하였으며, 각각의 절차에 따라 그림 5에서 보는 것처럼 정상적으로 인증이 가능한 것을 확인 할 수 있었다.

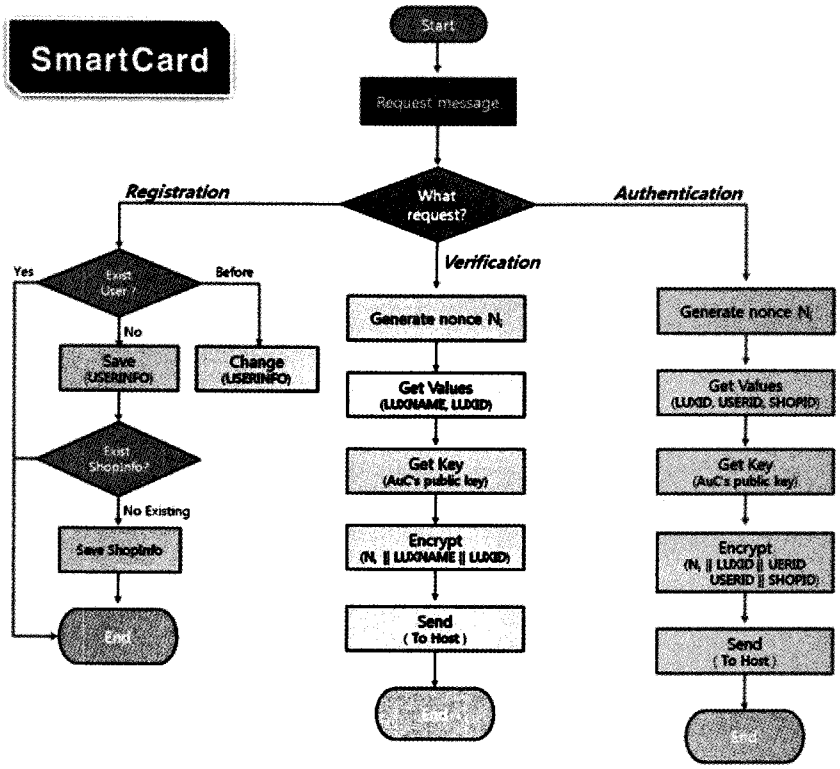

그림 4. 스마트 카드의 인증 흐름도

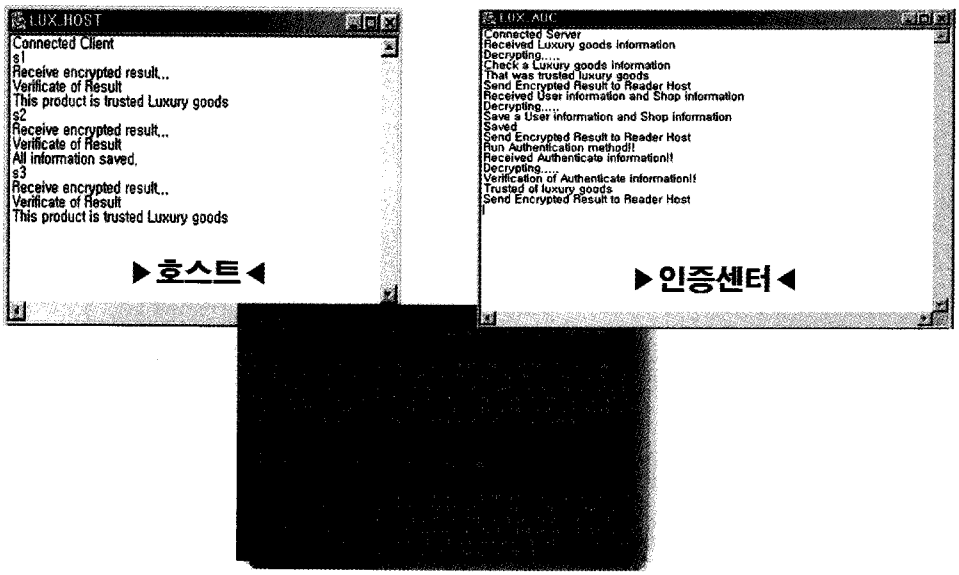

그림 5. 제안 시스템의 테스트 화면

5. 성능분석

본 논문에서는 제안하는 시스템을 크게 안전성과 효율성 측면에서 분석하였다. 안전성 측면에서는 기존 방식에서의 문제가 되었던, 재연공격과 인증 정보의 위조가 가능한지를 먼저 분석하였으며, 제안 방식

의 취약점이 될 수 있는 인증 정보가 저장된 파일 시스템에 대한 접근이 가능한지를 분석하였다. 그리고 효율성 측면에서는 제안 시스템과 기존 방식간의 효율성을 표로 비교 분석하였다.

5.1 안전성 분석

5.1.1 재연공격

본 논문에서 제안하는 인증 프로토콜 상에서의 노출되는 모든 정보는 기본적으로 인증 센터의 공개키로 암호화 되어 있다. 테스트에서 사용한 알고리즘은 RSA이며, 키의 크기는 1024bit를 사용하였다. 이때 단순히 인증 정보를 암호화만 하여 송신할 경우에는 스마트 카드와 호스트 그리고 호스트와 인증센터간의 통신단계에서 노출되는 정보를 획득하여 해당 정보를 그대로 이식하는 방식으로 위조상품의 생산이 가능하지만, 제안하는 방식에서는 매 인증 세션마다 다른 값을 송신하기 위하여 난수를 생성하여 해당하는 인증 정보와 연접 한 뒤 인증센터의 공개키로 암호화 하여 송신함으로서 전 단계에서 사용한 암호화된 정보를 사용하여 다음 단계에서의 인증 정보로 재 사용할 수 없어, 재연공격에 안전하다.

5.1.2 인증 정보 위조

본 논문에서의 인증 정보는 안전한 파일시스템에 저장되고 통신을 수행하는 과정에서는 안전한 공개키 기반 암호 알고리즘을 사용하여 수행한다. 이에 따라 인증 정보를 위조하기 위해서는 해당하는 공개키 기반 암호 알고리즘 자체를 공격해야하는데, 같지 않은 두 개의 큰 소수인 p와 q의 연산을 통해서 RSA 암호 알고리즘은 안전성을 확보한다. 일반적인 RSA의 속도와 관련된 알고리즘의 계산 복잡도를 살펴보면, 본 논문에서의 암호화 연산의 복잡도는 $O(1024^2)$, 복호화 연산은 $O(1024^3)$이고, 키 생성은 $O(1024^4)$이 되므로 사실상 인증 정보를 위조하는 것은 불가능 하다.

5.1.3 파일 시스템에 대한 직접 접근

제안 시스템에서의 인증정보는 파일 시스템에 저장 및 관리 된다. 이때 파일 시스템에서는 각각의 파일마다 Access Condition을 가지고 있으며 이때 파일에 대한 접근 조건을 설계에서는 PIN 검증을 통해서만 접근이 가능하도록 하였다. 그러므로 PIN 정보가 하드 코딩된 인증 애플릿을 제외한 다른 어떤 애플릿 또는 프로그램도 인증 정보가 저장된 파일에 접근 할 수 없도록 하여 저장 공간의 안전성을 확보할 수 있었다.

5.2 효율성 분석

본 논문에서 제안하는 방식과 기존 방식의 효율성은 표 1에서 보는 것과 같다. 제안방식의 경우에는 기존 방식과는 달리 양방향 인증을 수행함으로서 안전성이 높다. 그리고 활용방안은 다른 방식과 동일하게도 부착하는 형태이고, 데이터의 저장 위치는 전용 프로세서를 탑재한 Smart Card에 저장된다. 그리고 인증을 위한 인증 거리는 30Cm 이내로, 원거리에서 물품을 인증할 필요가 없으므로 적당하다. 그리고 비용은 가장 높은 편이지만, 위조품을 원천적으로 차단한다는 의미에서 1$의 내외는 그렇게 비싸지 않다고 할 수 있다.

그리고 제안 기법의 경우에는 기존 방식이 인증 정보만을 저장 하였다면, 제안 방식에서는 상품의 정

표 1. 기존방식과 제안 방식의 효율성 비교

	인증방식	활용방식	저장위치	인증거리	비 용
ID 기반	단방향	부착,소지	Label	식별가능 가시거리	가장저렴
바코드/ Smart tag	단방향	부착	Label	~30cm	저 렴
홀로그램	단방향	부착	Label	식별가능 가시거리	저렴~높음
RFID tag	단방향 (제한적 양방향)	부착	Tag	~100m	보통 (0.5~1$)
제안 기법	양방향	부착	SmartCard	~30cm	1$내외

보와, 판매점의 정보 그리고 개인의 정보를 저장 및 관리하여, 상품의 보증기간과 상품 이력 등을 추적할 수 있도록 하여, 다른 기존 방식에 비해 효율적이다.

6. 결 론

오늘날의 상품 시장을 해치는 가장 큰 요소는 바로 위조 상품들이다. 다양한 형태의 위조 상품들을 방지하기 위한 방법들이 제시되었으나, 위조 상품을 원천적으로 차단하기는 어려웠다. 이는 과거 스마트 카드의 단가가 RFID tag, 홀로그램 등에 비해 상대적으로 고가였으며, 카드의 성능 또한 우수하지 못하였기 때문에 사용자를 인증하거나 교통카드, 금융거래용도 등에 제한적으로 이용되었기 때문에, 위조품과 진품을 식별하기 위한 상품 인증 방식 운용을 목적으로 한 스마트 카드 활용 및 연구의 폭이 그리 넓지 않았다. 하지만 오늘날 스마트 카드의 단가는 저렴해 지고, 성능은 고강도 암호화 알고리즘을 탑재하여 상호인증 알고리즘을 운용할 수 있을 정도로 향상되었으며, 다양한 형태의 탑재 방식이 제안되어 일반 상품에 부착하여 제품을 인증을 용도로 활용할 수 있을 것으로 판단된다. 그러므로 본 논문에서는 기존 위조 방지를 위한 방식들의 가장 큰 문제점인 인증 정보의 노출을 원천적으로 차단하기 위하여 스마트 카드를 사용하여 안전하게 인증 정보를 관리할 수 있도록 하였다. 또한 스마트 카드에 대한 공격을 방어하기 위하여 먼저 스마트 카드 내에 안전한 파일 구조를 설계 및 구현하여, PIN 인증을 통과하여야만 해당 파일에 접근 할 수 있도록 하였으며, 상품과 리더(호스트), 그리고 리더와 인증센터간의 통신상에서의 노출은 난수와 1024bit의 RSA암호 알고리즘을 사용하여 인증 정보의 노출 없이 안전하게 통신을 수행하여 원천적으로 위조 상품의 발생을 차단할 수 있었으며, 다른 인증 방식에 비해 약간 높은 비용 외에는 다양한 정보의 저장으로 그 효율성이 높다.

참 고 문 헌

[1] 고정식, "지식재산권 집행 규범의 국제적 동향," 특허청, 제82권, pp. 3-10, 2008.

[2] 특허청, "위조상품 단속 매뉴얼," 특허청, 2006.

[3] 이윤석, 전하용, 이상용, 정민수, "명품인증을 위한 자바카드 파일 시스템 설계 및 구현," 한국멀티미디어학회 추계학술발표대회 논문집, 제12권, 제2호, pp. 167, 2009.

[4] 김은, 이윤석, 정민수, "자바 카드를 이용한 명품 인증 프로토콜 설계," 한국멀티미디어학회 춘계학술발표대회 논문집, 제13권, 제1호, pp. 19, 2010.

[5] 최영규, "블록 명암대비와 프로젝션에 기반한 2차원 바코드 검출 알고리즘," 정보처리학회논문지, 제15-B권, 제4호, pp. 259-268, 2008.

[6] D.Parikh, "Localization and Segmentation of A 2D High Capacity Color Barcode," Applications of Computer Vision, 2008. WACV 2008. IEEE Workshop, pp. 1-6, 2008.

[7] H.J. Kwon and T.H. Park, "An Automatic Inspection System for Hologram with Multiple Patterns," SICE Annual Conference 2007, pp. 2663-2666, 2007.

[8] 임지환, 오희국, 김상진, "동기화 문제를 해결한 새로운 동적 아이디기반 RFID 상호 인증 프로토콜," 정보처리학회논문지, 제15-C권, 제6호, pp. 469-480, 2008.

[9] 문미경, "RFID 애플리케이션 개발을 위한 태그 흐름기반 배치 시뮬레이터," 정보처리학회논문지 D, 제17권, 제2호, pp. 157-166, 2010.

[10] Z. Chan, *Java Card Technology for Smart Cards*, Addison-Wesley, 2000.

[11] 탁승호, 스마트카드, 성안당, pp. 94-100, 2004.

[12] 이윤석,전하용,정민수, "File Cache 및 Direct Access기능을 추가한 Java Card File System에 관한 연구," 한국멀티미디어학회논문지, 제11권, 제3호, pp. 404-413, 2008.

[13] 송영상, "자바카드 파일 시스템 API에 관한 연구," 단국대학교 대학원 박사학위 논문, 2007.

김 은

2009년 경남대학교 컴퓨터공학부 졸업(공학사)
2010년~현재 경남대학교 첨단공학과 석사과정
관심분야: Java Technology, Home Network Security, Network Security

이 윤 석

2006년 경남대학교 컴퓨터공학부 졸업(공학사)
2008년 경남대학교 컴퓨터공학과 졸업(공학석사)
2010년~현재 경남대학교 컴퓨터공학과 박사 수료
관심분야: Java Card, Mobile Security, Home Network Security

정 민 수

1986년 서울대학교 컴퓨터공학과 학사
1988년 한국과학기술원 전산학과 석사
1994년 학국과학기술원 전산학과 박사
1990년~현재 경남대학교 컴퓨터공학부 교수
관심분야: Java Technology, JavaMachine, Home Networking