Journal of Korea Multimedia Society Vol. 13, No. 2, February 2010(pp. 287-297)

자바카드를 이용한 서비스 기반 홈 디바이스 인증 기법에 관한 연구

이윤석[†], 김은[††], 이건혁[†††], 정민수[††††]

요 약

홈 네트워크 환경에서의 디바이스의 안전한 사용을 위해서는 인증이 필요하다. 이러한 인증은 크게 ID기반의 인증 방식과 인증서 기반의 인증방식이 있다, ID기반의 방식의 경우에는 멀티도메인 환경에 적용이 어렵고, 인증서 기반 방식의 경우에는 인증서를 탑재 및 저장하는 방식이 디바이스에 종속되어 있어, 소유권의 이전, 새로운 장비의 구매 등에 대한 사용자의 추가 설정이 요구된다. 그리고 두 가지 방식 모두 디바이스에 대한 개별적인 인증이 이루어져, 사용자가 요구하는 서비스 측면에서는 다수의 디바이스에 대한 잦은 인증으로 오버헤드가 존재한다. 이러한 문제를 해결하기 위하여 본 논문에서는 자바 카드에 디바이스 인증정보를 안전하게 저장 및 관리하는 기법을 제안하며 또한 서비스단위의 그룹기반의 디바이스 인증 기법을 사용하여 기존의 기법들에 비해 보다 향상된 수행속도를 보장한다.

A Study on Home Device Authentication method based service using Java Card

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

ABSTRACT

Authentication is needed to use safe devices in the home network environment. In this authentication, there are an ID base form and Certification base form. In case of an ID base form, it is difficult to apply to the multi domain environment and in case of an Certification base form, because the way that contains and stores the certificate demand on devices, additional setting of the user is needed for transfer of ownership and purchase of new devices, and more. Because both ways attend an individual authentication for devices, the ways exist overhead as the frequent authentication for a lot of devices in service aspects of user needs. To arrange these problems, in this paper, the authentication information of devices can be securely stored and managed in the java card and a processing time of the authentication could be improved better then the existing technique by authenticating a group of service.

Key words: Home Network(홈 네트워크), Device Authentication(디바이스 인증), Group Authentication (그룹 인증)

※ 교신저자(Corresponding Author) : 정민수, 주소 : 경남 마산시 월영동(631-701), 전화 : 010-6574-7633, FAX : 055)249-2647, E-mail : msjung@kyungnam.ac.kr
접수일 : 2009년 11월 18일, 수정일 : 2009년 12월 23일
완료일 : 2010년 1월 25일
[†] 준회원, 경남대학교 컴퓨터공학과 박사 수료
(E-mail : lysis2jt@yahoo.co.kr)
[††] 준회원, 경남대학교 첨단공학과 석사과정
(E-mail : sil7777@nate.com)
[†††] 준회원, 경남대학교 첨단공학과 석사과정
(E-mail : freedom6925@hanmail.net)
[††††] 종신회원, 경남대학교 컴퓨터공학부 교수
※ 본 연구는 2009년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2009-0067823)

1. 서 론

홈 네트워크 환경은 사용자의 서비스 요구에 따라 여러가지 동작을 수행하여야 한다. 사용자에게 제공되는 서비스는 단순히 하나의 디바이스에 대해 특정 동작이 요구되는 경우도 있으나, 실제 사용자 서비스의 관점에서는 여러 디바이스의 조합에 의해 발생한다[1,2]. 이는 사용자의 생활 패턴에 의해 주로 결정되어 지며, 사용자의 생활 패턴은 특별한 상황이 없는 한, 반복되는 경향을 가진다[1,2]. 예를 들면 저녁에 퇴근한 사용자가 집에 들어서면 자동으로 조명이 조절되고, 온수가 준비되며, 센서에 의한 감지로 사용자의 피로도를 확인 아로마 테라피 서비스도 가능하다. 이러한 일련의 과정들이 하나의 사용자의 요구 서비스라고 할 경우에 기존의 방식인 ID, 또는 인증서 기반의 경우에는 도어락, 조명, 온수 조절 시스템, 센서, 아로마 방향제 디바이스 등의 모든 디바이스에 대한 개별적인 인증의 수행으로, 사용자에 대한 서비스 제공 속도가 저하 될 수 밖에 없다. 그리고 ID기반의 경우에는 초소형 환경에도 쉽게 탑재되어 인증서 기반의 방식에 비해 고속의 처리가 가능하다는 상대적 이점이 있지만, 디바이스의 이전, 판매, 그리고 사용자의 이동에 따른 멀티도메인 환경에서는 인증정보를 저장 관리하는 것이 사실상 불가능하다[3]. 그리고 이러한 멀티 도메인 환경에서는 인증서 기반의 처리가 좋으나, 이는 앞선 시나리오에 따라 상대적으로 느린 공개키 기반 암호알고리즘을 사용하고, 인증서의 저장 및 관리가 어려우며, 역시 마찬가지로 그림 1에서와 같이 디바이스에 대한 개별적인 인증을 수행함으로 해서 서비스의 속도를 떨어뜨린다.

본 논문에서는 이러한 디바이스 중심의 개별적인 디바이스 인증의 단점을 해결하기 위하여 사용자 서비스 중심의 인증으로 관점을 달리하여 인증서 기반의 인증 구조와 각각의 디바이스를 서비스 단위로 그룹화 하여 인증을 수행함으로 해서 사용자의 요구 서비스에 최적화된 안전하고 빠른 인증기법을 제안한다.

2장 관련연구에서는 기존의 인증 방식과, 본 논문에서 제안하는 자바 카드 저장 및 관리 기법에 대해 언급하고, 3장에서는 제안하는 홈 디바이스 인증기법의 설계, 4장에서는 구현 결과에 따른 실험, 마지막으로 5장에서는 결론에 대해서 알아본다.

2. 관련연구

홈 네트워크의 디바이스들은 사용자의 요구에 따른 서비스를 제공해 주기 위해 존재한다. 이러한 디바이스들은 사용자의 생활과 밀접하게 관련이 있고, 이 때문에 사용자의 개인 프라이버시 또는 안전과 직접적으로 연관이 있다[1,2]. 이 홈 디바이스에 대한 접근은 홈 네트워크를 사용하는 사용자로부터 인증이라는 것을 통해서 정당한 디바이스 인지를 확인하는 절차가 필요하다[3-6]. 2.1 절에서는 ID 기반 디바이스 인증 기법에 대해 설명하고, 2.2 절에서는 인증서 기반 디바이스 인증기법에 대해 설명한다. 그리고 2.3절에서는 본 논문에서 제안하는 보안 칩으로서의 자바카드의 구조에 대해 간략하게 설명한다.

2.1 ID 기반 디바이스 인증 기법

ID 기반 디바이스 인증 기법은 홈 네트워크에 존재하는 각각의 디바이스에 ID가 부여되고 이 부여된 ID를 사용하여 디바이스를 구별하고 인증의 중요 요소로 활용한다. 이러한 ID 기반 인증 방법은 그림 2와 같다[7].

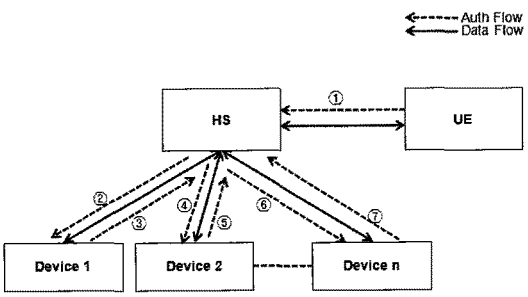

그림 1. 기존의 홈 디바이스 인증 기법

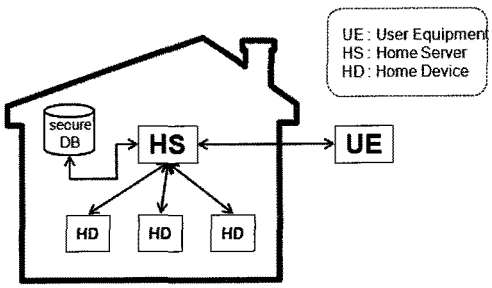

그림 2. ID 기반 홈 디바이스 인증 기법

그림 2에서처럼 홈 디바이스는 각각 ID를 할당받아 내부에 저장 하고 있고, 홈 서버는 이 모든 디바이스의 ID를 인식하고 있다. 사용자는 자신이 서비스 받기를 요구하는 홈 다바이스의 ID를 통해 접근을 시도하고, 홈 서버는 이를 인증하여 사용자가 홈 디바이스를 제어할 수 있도록 한다. 이러한 ID 기반의 인증방법의 장점은 주로 비밀키 방식을 사용하여 인증서 기반에 비해 암호 알고리즘이 빠르고 경량화가 가능하여 홈 디바이스에 탑재가 수월하다. 단점으로는 그림 2에서와 같이 홈 서버가 홈 디바이스의 ID를 모두 안전하게 관리하고 있어야 하며 비밀키 방식의 단점인 키 관리의 어려움이 발생한다. 또한 사용자의 관점에서 디바이스의 이동이나, 변경에 대처하는 절차가 복잡하다. 이와 같은 멀티 도메인 환경에서도 안전한 인증을 수행하기 위하여 인증서 기반 인증 방식으로 연구가 진행 되어져 오고 있다.

2.2 인증서 기반 디바이스 인증 방식

인증서기반 인증방식은 그림 3에서 보는 것과 같이 공인된 인증기관을 통해 인증서를 배포하고, 배포된 인증서는 홈 디바이스에 탑재되어 디바이스를 인증하는데 활용된다[3,4]. 이때 탑재되는 인증서의 프로파일은 X.509 version 3의 구조를 바탕으로하여 경량화 설계 되었다[3,4].

인증서기반의 인증에서는 최상위 인증기관에서 인증을 수행하므로 도메인이 변경되더라도 해당 디바이스에 대한 인증이 가능하다[3,4]. 이러한 형태의 인증 방법의 단점은 각각의 디바이스에 대해 인증서를 발급 관리해야 하는 문제와 이 인증서를 안전하게 보관해야 하는 문제가 있다. 그리고 인증서 기반이므로 상대적으로 비밀키 방식에 비해 느린 처리 성능으로 잦은 디바이스에 대한 인증은 서비스의 질을 떨어뜨리는 결과가 발생한다.

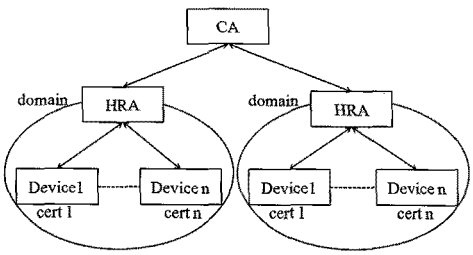

그림 3. 인증서 기반 홈 디바이스 인증 기법

2.3 자바 카드의 구조

자바카드는 스마트카드에 자바카드 가상기계(JCVM)를 탑재한 것이다[8]. 이 자바카드는 스마트카드와는 달리 애플릿 단위의 프로그램을 후 발급할 수 있는 장점이 있다. 자바카드의 환경은 그림 4와 같이 CPU와 RAM, ROM, 그리고 EEPROM/Flash memory로 구성되어 있다[8]. 이러한 형태의 자바카드는 물리적 공격에도 강하여, 전자여권, 교통카드, 금융 등 보안을 요구하는 여러 분야에 활용되고 있다. 이러한 자바카드는 현재 하드웨어 기반의 보안 장비들의 요구사항을 모두 만족하고 있으며, 초소형으로 휴대가 용이하고 탑재가 편리하다는 이점이 있다.

또한, 자바카드에는 다양한 애플릿이 후발급으로 탑재가 가능하여 사용자의 요구에 맞는 어플리케이션이 발급 이후에도 탑재가 가능하다[8]. 그리고 자바카드의 정보를 안전하게 저장 및 관리하기 위하여 자바카드에서는 ISO7816-4의 스마트 카드 표준에 따른 자바카드 파일 시스템이 탑재 가능하다. 그림 5는 ISO7816-4에 정의된 스마트카드 파일시스템의 구조이다[8].

Master File(MF)의 경우에는 특별한 형태의 Dedicate File(DF)로 루트 디렉토리에 해당한다. 그리고 DF는 일반적인 파일시스템의 디렉토리와 같은

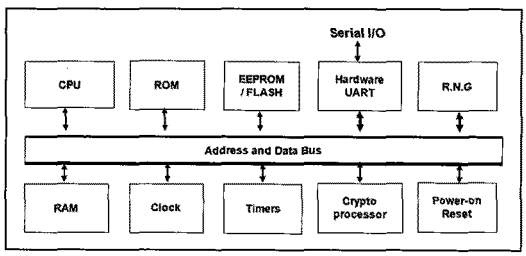

그림 4. 자바카드의 하드웨어 환경

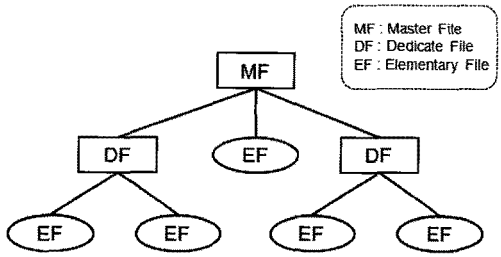

그림 5. ISO7816-4에 정의된 스마트카드 파일시스템

역할을 한다. MF와 DF는 정보를 가지지 않는다. 정보는 오직 Elementary File(EF)만 소유한다[8].

3. 제안 홈 디바이스 인증 기법

본 논문에서는 멀티 도메인 환경을 위한 인증서기반의 인증방식, 디바이스에 대한 그룹인증을 수행하기 위해 ID 기반 방식의 혼합 구조를 제안하고, 인증서 및 인증 정보를 안전하게 저장 및 관리하기 위해 자바카드를 홈 디바이스에 내장하는 방법에 대해서 제안한다. 먼저 3.1에서는 홈 디바이스에 저장될 정보들을 정의하고, 3.2에서는 정의된 정보를 저장 및 관리하기 위한 자바카드 구조를 설계하며, 3.3 에서는 저장된 정보를 활용하여 안전하고 효율적인 서비스 기반 그룹 인증 방식에 대해 설계한다. 그리고 3.4에서는 홈 디바이스에 자바카드가 탑재될 경우의 홈 디바이스와 자바카드 간의 필요 인터페이스에 관해 정의하였다.

3.1 홈 디바이스의 저장 정보 정의

효율적인 홈 디바이스의 인증을 수행하기 위해서는 먼저 홈 디바이스의 저장 정보를 정의하여야 한다. 본 논문에서는 그룹화된 인증을 수행하기 위하여 서비스에 따른 정보를 홈 디바이스의 상태정보, 홈 디바이스의 인증 정보, 홈 디바이스의 소유자 정보, 연관 디바이스 정보로 크게 4가지로 구분하였다. 먼저 홈 디바이스의 상태 정보는 사용자에게 서비스를 제공하기 위하여 디바이스는 자신의 현재 상태에 관한 정보이다. 그리고 홈 디바이스의 인증 정보는 홈 디바이스를 인증하기 위한 키 · 인증서 등의 인증정보 이며, 홈 디바이스의 소유자 정보는 홈 디바이스에 대한 소유자를 구분하기 위한 소유자 정보를 말한다. 이 소유자 정보의 경우에는 소유자에 따른 차등 서비스와 소유권 이전에 따른 소유자 정보의 추가 및 갱신이 원활한 구조로 저장되어야 한다. 그리고 연관된 디바이스 정보의 경우에는 사용자가 요구하는 서비스에 따라 서로 서비스로 연관된 디바이스들의 정보를 유지 관리함으로써 그룹화된 인증을 수행할 수 있도록 해준다.

3.2 홈 디바이스 인증 정보 저장구조

앞서 정의한 홈 디바이스의 정보들을 효율적으로 저장 및 관리하기 위해서는 파일 시스템이 필수적이다. 파일시스템은 파일에 대한 접근을 차등적으로 제공할 수 있으며, 기존에 탑재된 애플릿의 업그레이드 시에도 자료를 안전하게 유지 관리 할 수 있다.

본 논문에서는 안전한 정보의 저장 및 관리를 위하여 그림 6과 같은 형태로 파일 구조를 구성하였다.

먼저 파일을 식별하기 위하여 각각의 파일에는 파일 식별자(FID)를 할당하였다. ISO7816-4의 표준에 따라 최상위의 MF의 FID를 '3F00'로 하였으며 이후 홈 네트워크를 관리하는 DF로 '7F00'의 파일을 생성하였다. 그리고 그 하위에 아래의 3종류의 파일을 생성하여 디바이스의 상태정보, 소유자 정보, 디바이스의 인증정보, 연관 디바이스 정보를 저장 및 관리한다. 각각의 파일은 그림 7에서와 같이 TLV (Tag, Length,Value)의 형태로 구성된다.

이러한 TLV 구조는 각각의 정보를 구별할 수 있는 Tag와 길이 정보만 있으면 얼마든지 확장이 가능

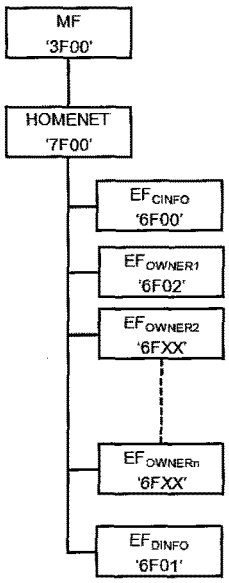

그림 6. 제안 자바카드 파일 구조

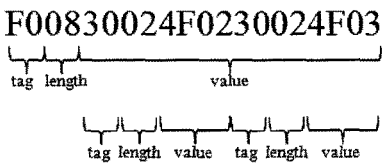

그림 7. TLV 구조의 예

표 1. TAG와 해당 값

TAG explain	TAG value	Use file
Field	F0	All
EFowner file	30	6F00
Device ID	00	6F01,6F02
IP Address	01	6F01
Owner ID	10	6F02
Owner SK	11	6F01
Owner IK	12	6F01
Owner Certificate	20	6F01
Device State	30	6F01

하다는 장점이 있다. 본 논문에서 제안하는 기법은 다양한 디바이스들이 연관성을 확인하여 서로 연결되는 구조로서, 지속적으로 확장 될 가능성이 있기 때문에 이와 같은 TLV 구조로 정보를 저장 및 관리하는 것이 중요하다.

표 1은 본 논문에서 제안하는 TLV 파일 구조에서 태그에 대한 설명과 그 값을 보여준다. 필드 태그의 경우에는 모든 파일에서 사용되며, 각각의 필드들을 구분한다. EFowner 파일 태그는 CINFO파일에서 사용되며 소유자 파일을 구분하는 태그이다. Device ID 태그는 EFowner, DINFO 파일에서 사용되며 소유자가 소유한 디바이스의 ID를 나타낸다. IP 주소 태그의 경우에는 DINFO 파일에서 사용되며 해당 디바이스의 IP 주소를 나타낸다. Owner ID 태그는 DINFO파일에서 사용되며 디바이스의 소유자 정보를 나타내고 이에 따라 종속된 소유자의 키 정보를 관리하는 태그인 Owner SK , Owner IK 태그, 그리고 소유자의 인증서를 저장하는 Owner Certificate 태그가 뒤이어 나온다. 그리고 Device State 태그는 DINFO 파일에서 사용되며 디바이스의 상태를 저장한다. 이러한 형태의 태그 정보를 각각의 파일에서 저장 및 관리한다.

3.2.1 CINFO

이 파일의 FID는 '6F00'이며, 이 파일은 EFowner 파일을 관리한다. 디바이스는 다수의 사용자가 존재할 수 있으며 각각의 접근 방법에 따른 제어 정보가 상이하므로 이를 위해서는 사용자 별로 파일을 생성하여 관리하는 것이 필요하다. CINFO 파일에서는 사용자의 확장성을 고려하여 소유자 정보 파일을 관리하는 파일이다.

3.2.2 EFowner

이 파일의 FID 는 '6F02'이며, 이 파일은 소유자의 정보를 저장 및 관리한다. 이 파일에서는 소유자와 소유한 디바이스를 나타내고 있어, 디바이스에 대해 접근할 수 있는 사람을 제한할 수 있다.

3.2.3 DINFO

이 파일의 FID는 '6F01'이며, 이 파일은 디바이스의 정보를 저장 및 관리한다. 이 파일에서는 디바이스의 상태 정보를 저장 하고 또한 디바이스를 인증하기 위한 키와 인증서를 저장 및 관리한다. 그리고 그룹화된 서비스를 제공하기 위해 연관된 디바이스의 IP 정보를 가지고 있어, 연관된 디바이스의 인증이 가능하도록 하였다.

3.3 제안 인증 기법

본 논문에서는 디바이스에 대한 개별적인 인증이 아닌, 사용자의 관점에서 사용자가 요구하는 서비스 단위로의 인증을 수행하도록 하는 그룹 인증을 수행하는 그림 8과 같은 기법을 제안한다.

인증의 수행순서는 크게 3부분으로 나누어 진다. 먼저 사용자 장비와 홈 서버 간의 인증이 있다. 이 과정에서 사용자 인증이 필요하고, 이후 홈 서버와 디바이스 간의 디바이스 인증이 필요하다. 그리고 마지막으로 디바이스와 디바이스 간의 인증이 이루어지는데, 각각의 절차는 다음과 같다.

먼저 인증은 다른 도메인의 디바이스인지를 확인한다. 이때 다른 도메인의 경우에는 인증서 기반 인증을 수행하여 멀티 도메인 환경에서도 안전하게 동

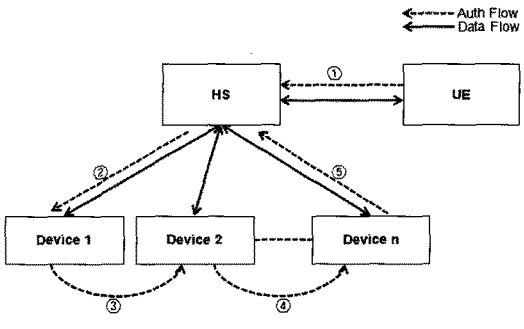

그림 8. 서비스 기반 그룹화 된 디바이스 인증 기법

작할 수 있도록 하였으며, 다른 도메인이 아닌 경우에는 ID기반의 인증을 수행한다. 그 첫 번째로 홈 서버와 사용자 간의 사용자 인증을 수행하게 되는데, 이 방식은 아래와 같다.

step 1 : 사용자는 홈 서버에 접속하여 난수 R_{HS} 생성을 요청한다.

step 2 : 홈 서버는 난수 R_{HS}을 생성하여 사전에 분배된 홈서버의 비밀키 K_{HS}로 난수 R_{HS}를 암호화 하여 사용자에게 송신한다.

step 3 : 사용자는 홈 서버로부터 수신한 정보를 홈 서버의 비밀키 K_{HS}로 복호화 하여 난수 R_{HS}를 획득하고, 사용자는 자신의 난수 R_{UE}를 생성하여 홈 서버가 생성한 난수와 연접 R_{HS}'||R_{UE}하여 홈서버의 비밀키 K_{HS}로 암호화 한 후 홈 서버에게 송신한다.

step 4 : 홈 서버는 수신된 정보를 자신의 비밀키 K_{HS}로 복호화 하여 자신이 송신한 난수 R_{HS}와 수신된 R_{HS}'을 비교하여 자신의 비밀키를 소유한 사용자임을 인증한다. 그리고 홈 서버는 세션키 SK를 생성하여 사용자가 생성한 난수 R_{UE}와 함께 연접 R_{UE}'||SK를 수행하여 사용자에게 송신한다.

step 5 : 사용자는 정보를 K_{HS}로 복호화 하여 자신이 생성한 난수 R_{UE}와 R_{UE}'이 동일한지를 확인하고 동일할 경우에는 공통된 홈 서버의 키 K_{HS}를 보유한 것으로 홈서버를 인증한다. 그리고 함께 수신된 SK를 통하여 이후 통신과정에서는 모두 세션키 SK를 통하여 암·복호화를 수행한다.

그리고 두 번째로 홈 서버와 홈 디바이스 간의 인증은 사용자와 홈 서버간의 인증스텝과 유사한 형태로 단지 난수를 생성하고 사용하는 주체가 홈서버와 홈 디바이스로 변경되었을 뿐이다. 이에 대한 설명은 아래와 같다.

step 1 : 홈 서버는 사용자의 요청된 서비스에 따라 주 가 되는 홈 디바이스 접속하여 난수 R_{HD} 생성을 요청한다.

step 2 : 홈 디바이스는 난수 R_{HD}를 생성하여 사전에 분배된 홈 서버의 비밀키 K_{HS}로 난수 R_{HD}를 암호화 하여 홈 서버에게 송신한다.

step 3 : 홈 서버는 홈 디바이스로부터 수신한 정보를 홈 서버의 비밀키 K_{HS}로 복호화 하여 난수 R_{HD}를 획득하고, 홈 서버는 자신의 난수 R_{HS}를 생성하여 홈 서버가 생성한 난수와 연접 R_{HD}'||R_{HS}하여 홈 서버의 비밀키 K_{HS}로 암호화 한 후 홈 디바이스에게 송신한다.

step 4 : 홈 디바이스는 수신된 정보를 비밀키 K_{HS}로 복호화 하여 자신이 송신한 난수 R_{HD}와 수신된 R_{HD}'을 비교하여 공유된 비밀키를 소유한 홈 서버임을 인증한다. 그리고 홈 디바이스는 인증이 이루어졌음을 알리는 SF와 R_{HS}'을 연접 R_{HS}'||SF를 비밀키 K_{HS}를 통하여 암호화 하여 송신한다.

step 5 : 홈 서버는 정보를 K_{HS}로 복호화 하여 자신이 생성한 난수 R_{HS}와 R_{HS}'이 동일한지를 확인하고 동일할 경우에는 공유된 홈 서버의 키 K_{HS}를 보유한 것으로 홈디바이스를 인증한다. 그리고 이후 사용자와 공유된 SK를 SF'와 연접 SF'||SK을 공유된 홈 서버의 키 K_{HS}를 통하여 암호화 후 송신한다.

위의 단계에서 와 같이 홈 서버와 사용자 장비간의 인증은 난수 교환에 의한 상호 인증을 수행한 뒤 세션키 일치 과정을 거친다. 이러한 방식으로 일치된 세션키는 향후 세션이 종료되기 전까지 동일한 키를 사용하므로 안전하고, 효과적으로 인증을 수행하게 된다. 그리고 마지막 인증인 디바이스와 디바이스 간의 인증은 그림 9에서 보는 것과 같다. 먼저 앞선 위의 단계에서와 같이 연관된 디바이스 중에 주 가 되는 홈 디바이스와의 상호 인증과 세션키 일치 이후에는 주 가 되는 홈 디바이스는 자신의 연관 테이블을 검색하여 해당하는 디바이스에 접속한다. 이후 홈 서버에서 생성한 난수와 자신의 ID를 해쉬하여 연관된 디바이스에 송신하게 된다. 이와 관련된 방식은 아래와 같다.

step 1 : 주 가 되는 홈 디바이스는 홈 서버로부터 수신된 난수 R_{HS}와 자신의 디바이스 ID인 DevID1을 연접하여 해쉬 함수를 사용하여 해쉬한다. 그리고 이

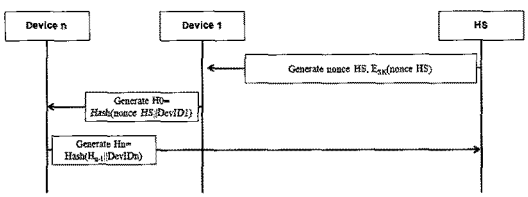

그림 9. 서비스별 그룹화된 디바이스와 홈서버간의 인증 프로토콜.

정보는 서비스를 제공하기 위해 연관된 홈 디바이스에 송신한다.

step 2 : 종 이 되는 홈 디바이스는 주 홈 디바이스로부터 수신된 정보에 자신의 다바이스 ID인 DevIDn을 연접하여 연관된 디바이스에 송신한다.

이와같이 위의 2 스텝을 반복하여 서비스를 중심으로 그룹화된 모든 디바이스의 ID가 해쉬되고 최종적으로 마지막 디바이스는 홈 서버에 그 정보를 송신한다. 그리고 그림 9와 같이 서비스를 중심으로 한 디바이스 그룹에 대한 인증은 해쉬 체인 기법이 핵심적이다. P를 해쉬 함수를 수행한 결과라고 하고 ID를 디바이스 ID, 그리고 h를 해쉬함수라고 하였을 때 이러한 인증 방법은 아래와 같다[9].

$$P_0=h^N(ID) \quad (1)$$

다음 해쉬 함수의 수행결과는 아래와 같다.

$$P_1=h^{N-1}(ID) \quad (2)$$

이를 정규식으로 표현하면

$$P_i=h^{N-i}(ID) \quad (3)$$

N은 해쉬 함수의 수행횟수를 뜻하고 이는 서비스를 제공하기 위해 그룹화된 홈 디바이스의 개수를 말한다.

이를 검증하는 홈 서버는 아래와 같은 식에 의해서 검증을 수행한다.

$$P_i=h(h^{N-i-1}(ID))=h(P_{i+1}) \quad (4)$$

이를 통해서 해쉬 된 내용을 검증하고 이에 대한 안전성은 해쉬 함수가 가지는 안전성이다.

3.4 자바카드와 홈 디바이스간의 통신 구조

제안하는 인증 기법은 홈 디바이스에 자바카드 칩이 탑재되어 안전하게 인증 정보를 저장 및 관리 할 수 있는 형태의 구조이다. 이러한 형태의 인증 정보를 저장 및 관리하기 위해서는 홈 디바이스와 자바카드 칩 간의 공통된 통신 방식과 관리 메소드가 필요한데, 이에 따라 그림 10과 같이 설계 하였다.

그림 10에서 보는 것과 같이 자바카드 칩내에는 자바카드 가상기계와 암호화 API 그리고 자바카드 파일 시스템이 탑재되고 이와 관련된 내용은 앞서 설명하였다. 그리고 각각의 홈 디바이스와 관련

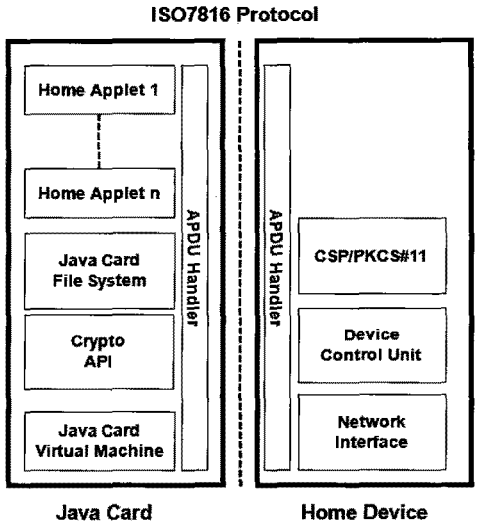

그림 10. 자바카드와 디바이스간의 통신

된 특정 서비스를 제공하기 위한 애플릿들이 탑재된다. 이러한 애플릿에 대한 접근은 홈 디바이스와 자바카드간의 ISO7816-4 표준에 따른 APDU 통신 프로토콜을 사용한다. 이를 위해 APDU 핸들러가 필요하고 홈 디바이스에는 네트워크와 연결되어야 하므로 네트워크 인터페이스, 그리고 디바이스를 제어해야 하므로 제어 유닛과 멀티 도메인 환경에서도 동작하기 위하여 CSP/PKCS#11의 인증서 관리 메소드가 필요하다.

4. 실험 및 분석

본 논문에서의 개발 및 테스트 환경은 32bit 프로세서 및 토네이도2 암호전용 프로세서가 탑재된 S3FJ9SK 보드를 사용하였으며 개발 툴로는 ARM Developer Suite V1.2를 사용하여 개발하였다. 에뮬레이터로는 OpenICE-A1000을 사용하였다. 암호화 알고리즘으로는 AES를 사용하였고, 해쉬 함수로는 SHA1을 사용하였다. 인증서를 통한 인증 부분은 실험에서 고려하지 않았다. 그리고 실험을 위해 루프백 주소로 연관 디바이스 정보를 저장하여, 해쉬 함수를 통한 인증이 가능하도록 하였다. 실험 결과에 따른 분석은 크게 안전성과 효율성으로 나누어 분석하였으며, 안전성 부분에서는 인증프로토콜 상의 안전성과 인증정보 관리기법의 안전성을 분석하였고, 효율성 부분에서는 자바카드를 통해 인증정보를 저장 및

관리함으로서 발생하는 효율성과, 제안하는 서비스 기반 인증 기법의 수행성능에 대한 효율성을 비교 분석하였다.

4.1 안전성 분석

먼저 홈 네트워크에는 사용자 단말과 홈 서버 그리고 홈 디바이스로 구분되는 일련의 장비들이 인증을 통해서 안전하게 수행되기를 원한다. 본 논문에서는 먼저 이러한 인증 방식에서 홈 서버와 홈 디바이스간의 인증을 중심으로 분석해 보았다.

4.1.1 인증 프로토콜의 안전성 분석

본 논문에서 제안하는 방식과 기존의 ID기반 방식, 인증서 기반 방식의 인증 프로토콜 상에서 발생할 수 있는 몇 가지 문제점을 표 2에서와 같이 분석하였다.

표 2에서 처럼 ID기반 방식의 경우에는 중간자 공격에 취약하다. 이는 단순한 ID의 사용에 의해서 디바이스에 대한 중간자 공격이 가능하고, 재연공격 역시도 난수를 활용한 암호 프로토콜이 사용되지 않을 경우에는 언제든지 재연공격이 가능하다는 취약점이 발생한다. 그리고 인증 정보가 단순한 ID 기반이고, 홈 디바이스에 탑재되어 있어 이 정보를 가공하는 보안 프로세서의 부재로 인해서 인증 정보에 대한 직접적인 공격이 가능하다. 그리고 인증서 기반의 인증 방법의 경우에는 공개키 기반 방식으로 중간자 공격과 재연공격에 강하다. 하지만 인증서를 발급받고 인증 센터를 통해 인증하는 형태로 인증을 수행함으로 해서 발생하는 인증지연의 문제가 발생한다.

표 2. 안전성 분석

	ID based	PKI based	Suggest method
중간자 공격	O	X	X
재연공격	O	X	X
인증정보공격	O	O	X
인증정보 노출	O	O	X

본 논문에서 제안하는 방식은 난수교환에 의한 홈 서버와 사용자 단말간의 상호 인증이 이루어지므로 중간자 공격 및 재연공격에 강하고, 역시 홈 서버와 홈 디바이스간의 인증 역시도 난수의 교환에 의한 인증을 수행하므로 해서 중간자 공격 및 재연 공격에 강한 특성을 가지고 있다.

4.1.2 인증정보 관리기법의 안전성 분석

본 논문에서 제안하는 인증 정보는 물리적 공격에 강한 스마트카드에 자바 가상기계를 탑재한 자바카드로, 인증 정보는 이 자바카드에 안전하게 저장 및 관리된다. 이는 기존의 단순 ID 기반 방식에서 발생하였던, 인증 정보인 ID가 홈 디바이스에 탑재되어 홈 디바이스에 대한 직접 접근 또는 인증 프로토콜 상에 발생되는 노출에 의해 공격이 이루어지는 것을 방지 할 수 있으며, 또한 인증서 기반의 인증 기법에서 역시 마찬가지로 표 2에서 보는 것과 같이 인증서를 자바카드에 안전하게 저장 및 관리함으로써 기존의 방식에서 제공되지 않는 인증 정보의 안정성을 확보한다.

4.2 효율성 분석

4.2.1 자바카드를 이용한 인증 방식의 효율성 분석

본 논문에서는 표 3에서와 같이 ID기반 그리고, 인증서 기반과 비교하여보면, ID 기반의 경우에는 인증 정보가 ID로 단순하여 인증서기반 방식에 비해서는 고속의 처리가 가능하다. 하지만 멀티 도메인 환경에서의 처리는 인증을 수행 할 수 있는 인증 서버의 구성이 불가능하여 멀티 도메인 환경에서의 처리가 어려운 단점 이 있으나, 인증을 그룹화 하여 인증을 수행 할 수 있다. 그리고 인증서기반 방식의 경우에는 인증서 기반의 인증 구조로 멀티 도메인 환경에 동작을 수행할 수 는 있으나, X.509v3 기반의 인증 프로파일의 일부를 수정하지 않는 한, 그룹 정

표 3. 효율성 분석

	인증 정보	멀티 도메인	그룹 인증	인증정보저장위치
ID 기반	ID	X	O	디바이스
인증서 기반	Certificate	O	X	디바이스
제안 기법	ID, Certificate	O	O	자바카드 칩

보를 저장 및 관리하는 것은 불가능 하다. 그리고 이 두 가지 방식은 인증 정보를 디바이스가 가지고 있어서 디바이스의 소유의 이전, 새로운 디바이스의 구매에 따른 새로운 인증서 발급 및 관리에 발생하는 문제와 오버헤드는 고려하지 않고 있다. 즉 이러한 문제는 디바이스의 관점에서 설계된 인증 기법의 한계로, 사용자의 서비스를 제공하는 서비스 관점에서의 인증에는 알맞지 않다.

본 논문에서 제안하는 기법의 경우에는 주요 인증 정보로는 ID 기반으로 단순화 하여 고속의 인증 방법을 수행하고, 멀티 도메인 환경에서는 인증서를 통한 인증을 수행한다. 그리고 그룹을 통한 인증으로 사용자 서비스 중심의 인증이 가능하도록 하였으며, 인증 정보의 저장 위치 역시 자바카드로 디바이스의 소유자가 변경되거나, 새로운 디바이스를 구매하여도 기존의 정보를 유지하고자 하는 사용자 중심의 관점에서 효율적으로 설계되었다.

4.2.2 제안 기법의 인증 횟수의 비교

그림 1에서와 같이 하나의 디바이스에 개별적인 인증을 수행하는 방식의 경우에 N을 디바이스의 개수라 하고, T_{HD}를 홈 디바이스 인증 시간, T_{HS}를 홈 서버 인증 시간, T_{UE}를 사용자 단말 인증 시간이라 할 경우에는 개별 홈 디바이스에 대한 인증은 인증을 위해 왕복으로 인증정보를 교환해야 하며, 이는 아래 식 (5)에서 보는 것과 같이 하나의 서비스 관점에서 묶여진 홈 디바이스의 개수 N의 배 만큼 시간이 증가한다. 그리고 홈 서버와 사용자 단말의 인증 시간은 이러한 홈 디바이스 당 인증 시간에 각각 더해져서 최종적으로 하나의 서비스를 제공하기 위한 모든 디바이스와 홈 서버 사용자 단말까지의 인증시간이 이루어지는데, 사실상 그림 1에서와 같은 기존의 방식에서는 사용자에게 하나의 서비스를 제공하기 위한 디바이스들의 개수에 수행 시간은 종속되어 있음을 아래 식 (5)에서 보는 것과 같다.

$$N(T_{HD} \times 2)+T_{HS}+T_{UE} \quad (5)$$

그리고 본 논문에서 제안하는 그룹화된 인증 기법의 경우에는 아래와 같다.

$$(N+1+T_{HD}')+T_{HS}+T_{UE} \quad (6)$$

그림 8에서 보는 것과 같이 개별 홈 디바이스를 인증하는 데 있어서 인증 정보를 상호 교환할 필요가 없고, 위의 식 6에서 보는 것과 같이 인증의 수행 시간이 앞선 (5)의 방식에 비해 노드의 개수만큼 배로 증가하는 것이 아닌 노드의 수 만큼 해쉬 한 결과를 전송하게 되므로 인증 시간이 줄어들고, 홈 디바이스의 인증 시간인 T_{HD} 역시도 암호화 보다 상대적으로 수행속도가 빠른 해쉬를 사용하여 (5)의 방법에 비해 T_{HD}' 역시 수행 속도가 향상되었음을, 그림 11과 같이 확인 할 수 있었다.

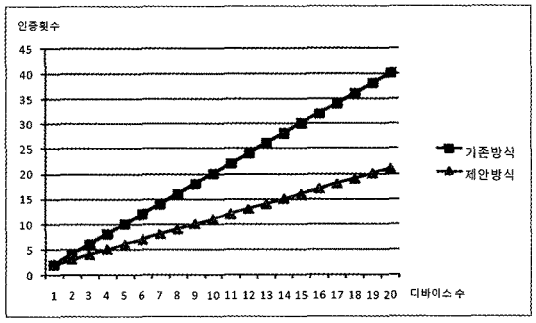

그림11. 기존 방식과 제안 방식의 디바이스 수에 따른 인증 횟수 비교

그림 11과 같이 기존의 방식은 디바이스 수에 비례하여 크게 증가하였던 반면에 제안 방식의 경우에는 기존 방식에 비해 인증 횟수가 적게 되어 인증의 반복에 의한 오버헤드를 감소시킬 수 있다. 그리고 제안 방식은 인증할 디바이스의 수가 증가 하면 증가할수록 그 성능이 기존 방식에 비해 향상됨을 확인할 수 있었다.

5. 결 론

홈 네트워크 환경은 사용자 중심의 환경으로 사용자는 사용자가 요구하는 서비스를 다양한 디바이스로부터 제공 받기를 원한다. 이러한 홈 네트워크의 환경에서 기존의 논문에서는 사용자 중심의 관점 보다는 디바이스 중심의 관점에서 안전성을 확보하기 위한 연구가 주를 이루었다. 하지만 이러한 관점의 문제는 사용자의 생활 패턴과 사용자의 서비스 요구에 최적화 되지 않아 다수의 인증을 통한 오버헤드가 존재하는 단점, 그리고 디바이스 이전 및 새로운 디바이스의 구매에 대한 설정 방법이 불편하다는 단점이 존재한다. 사용자 중심의 서비스 기반 구조에서 기존의 연구에 의한 인증 기법을 적용하면, 통신 오버헤드가 발생하고, 안전성 측면에서도 취약성이 발

생한다. 본 논문에서는 이러한 문제를 해결하기 위하여, 디바이스의 중요 인증정보는 자바카드에 탑재하여 이 자바카드가 홈 디바이스에 장착, 보안 칩으로서의 역할을 수행하고, 홈 서버에서는 사용자 중심의 서비스 그룹별로 인증을 수행하도록 하여, 사용자의 서비스 요구에 오버헤드 없이 인증을 수행할 수 있도록 하였다. 그리고 사용자의 소유권의 이전, 디바이스의 구매에 따른 설정의 불편함은 자바카드 칩 만을 교체 하여 탑재함으로서, 기존의 정보를 유지 할 수 있고, 소유권의 이전에도 활용할 수 있다.

참 고 문 헌

[1] R. Suzuki, M. Ogawa, Y. Tobimatsu, and T. Iwaya, "Time-Course Action Analysis of Daily Life Investigations in the Welfare Techno House In Mizusawa," *Telemedicine Journal and e-Health*, Vol.7, 2001.

[2] T. Tamura, T. Togawa, M. Ogawa, and M. Yoda, "Fully automated health monitoring system in the home," *Medical Engineering & Physics*, Vol.20, 1998.

[3] D. G. Lee, G. W. Kim, J. W. Han, Y. S. Jeong, and D. S. Park, "Smart Environment Authentication:Multi-Domain Authentication, Authorization, Security Policy for Pervasive Network," UMC' 08, pp.99-104, 2008.

[4] Y. K. Lee, D. G. Lee, J. W. Han, and T. H. Kim, "Home Network Device Authentication :Device Authentication Framework and Device Certificate Profile." *Computer Journal.Oxford University*, July 2008.

[5] M. Hirano, T. Okuda, and S. Yamaguchi, "Application for a Simple Device Authentication Framework:Device Authentication Middleware using Novel Smart Card Software," SAINT-W 2007, pp.31-34, 2007.

[6] J. P. Jeong, M. Y. Chung, and H. S. Choo, "Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks System," HICSS 2008, pp. 294-300, 2008.

[7] K. V. Nguyen. "Simplifying Peer-to-Peer Device Authentication Using Identity-Based Cryptography," ICNS' 06, pp. 43-47, 2006.

[8] W. Rankl, and W. Effing, "*Smart Card Handbook*," JOHNWILEY & SONS, 2003.

[9] K. Bicakci, and N. Baykal, "Infinite Length Hash Chains and Their Applications," WET ICE 2002, pp. 57-61, 2002.

이 윤 석

2006년 경남대학교 컴퓨터공학부 졸업(공학사)

2008년 경남대학교 컴퓨터공학과 졸업(공학석사)

2010년~현재 경남대학교 컴퓨터공학과 박사 수료

관심분야 : Java Technology, Java Card, HomeNetwork Security

김 은

2009년 경남대학교 컴퓨터공학부 졸업(공학사)

2010년~현재 경남대학교 첨단공학과 석사과정

관심분야 : Java Technology, Java Card, HomeNetwork Security

이 건 혁

2009년 경남대학교 컴퓨터공학부 졸업(공학사)
2010년~현재 경남대학교 첨단공학과 석사과정
관심분야 : Java Technology, Java Card, HomeNetworking

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