홈 네트워크 환경에서 OTA(One Time Authentication)키를 이용한 DA_UDC(Double Authentication User · Device · Cross) 모듈 설계

정회원 정 은 희*, 이 병 관**

A Design of DA_UDC(Double Authentication User · Device · Cross) Module using OTA(One Time Authentication) Key in Home Network Environment

Eun-Hee Jeong*, Byung-Kwan Lee** *Regular Members*

요 약

본 논문에서는 OTA(One Time Authentication)키를 이용한 사용자 인증, 디바이스 인증 그리고 상호 인증 모듈을 사용하여 공인인증서 비용과 도용문제를 해결하고, 홈 네트워크 사업자의 서비스에 가입할 필요가 없는 이중 인증 기법인 DA-UDC(Double Authentication User · Device · Cross) 모듈을 설계하였다. 홈 서버는 사용자 아이디, 디바이스 아이디 그리고 세션키를 확인하는 1단계 인증 과정을 통과한 사용자에 대해 OTA키 생성에 필요한 홈 서버 공개키를 전송하고, 사용자가 생성한 OTA키를 확인하는 2단계 인증과정을 수행한다. 이때 생성되는 DA-UDC 모듈의 OTA키는 생성될 때마다 변경되도록 설계하였다. 따라서 DA-UDC 모듈은 이중 인증 과정을 수행함으로써 사용자 아이디 및 디바이스 아이디 노출을 대비하였고 OTA키 사용으로 악의의 사용자로부터 홈 네트워크의 인증 보안을 강화시켰다. 또한, DA-UDC 모듈은 단 1회의 인증 연산 횟수를 가지므로 기존의 인증 시스템보다 처리 속도가 빠르며, 별도의 인증키를 사용하므로 데이터 전송량은 많지만 보안측면에 강화시켰다고 볼 수 있다.

Key Words : User Authentication, Device Authentication, Cross Authentication, OTA(One Time Authentication) Key, Double Authentication

ABSTRACT

This paper propose DA-UDC(Double Authentication User, Device, Cross) Module which solves the cost problem and the appropriation of Certificate using User Authentication, Device Authentication and Cross Authentication with OTA(One Time Authentication) Key, and which is designed not to subscribe to the service of Home network business. Home Server transmits its public key which is needed to create OTA to the user which passed the first step of authentication which verifies User ID, Device ID and Session Key. And it performs the second step of authentication process which verifies the OTA key created by a user. Whenever the OTA key of DA-UDC module is generated, the key is designed to be changed. Therefore, DA-UDC Module prevents the exposure of User and Device ID by performing the two steps of authentication and enhances the authentication security of Home Network from malicious user with OTA key. Also, DA-UDC Module is faster than the existing authentication system in processing speed because it performs authentication calculation only once. Though DA-UDC Module increases data traffic slightly because of the extra authentication key, it enhances the security more than the existing technique.

* 강원대학교 지역경제학과 (jeongeh@kangwon.ac.kr), ** 관동대학교 컴퓨터학과 (bklee@kwandong.ac.kr)
논문번호 : KICS2008-12-535, 접수일자 : 2008년 12월 2일, 최종논문접수일자 : 2009년 1월 30일

Ⅰ. 서 론

최근 컴퓨터 및 정보통신 기술의 발달과 함께 급속히 발전하는 인터넷 기술은 저속 데이터 서비스는 물론 인터넷 폰, 전자신문, 주문형 비디오, 웹 TV 등 다양한 멀티미디어 서비스를 가능하게 하였다. 이러한 인터넷의 발전은 가정 내의 정보화도 가속시키고 있으며, 홈 네트워크 발전에 큰 영향을 주었다.

현재 홈 네트워크는 여러 분야의 기술들을 유기적으로 결합하여 사용하고 홈 네트워크의 특성상 다양한 종류의 디바이스가 통합된 네트워크 환경에서 제공되기 때문에 기존의 네트워크 환경에서 가지고 있던 보안 위협뿐만 아닌 새로운 형태의 보안 위협들이 증가하고 있는 추세이다. 이러한 보안 위협으로부터 안전한 홈서비스를 보장하기 위한 보안 요구는 날로 증대되어 보안 연구의 중요성을 부각시키고 있으며 그중에서도 사용자의 개입을 최소화하고 디바이스 상호간의 원활히 연동되는 홈서비스를 제공하기 위해서는 홈 네트워크 구성요소인 디바이스 인증이 필수적이다. 하지만, 디바이스 인증에서 X.509 기반의 인증서를 사용하거나 보안성만을 고려하여 복잡한 암호 알고리즘을 사용하기 때문에 고사양의 컴퓨팅 파워를 가진 디바이스 사양을 요구한다. 이로 인하여 저사양의 홈 디바이스에서는 계산에 한계를 가지고 있어 홈 네트워크 환경에서는 적용이 어렵다[1,2,3]. 따라서 홈 네트워크 서비스의 편리성과 안전성을 동시에 만족시키며, 기존 홈 네트워크 서비스 시스템에 용이하고 유연하게 적용할 수 있는 통합 보안 인프라 구축이 필요하다.

본 논문에서는 공인 인증서나 사설 인증서를 사용하지 않고 OTA(One Time Authentication) 키를 생성하여 서버가 사용자의 신분을 인증하고 디바이스를 인증하고 상호 인증을 할 수 있는 이중 인증 기법인 DA-UDC 모듈은 설계한다. DA-UDC 모듈이 설치된 홈 서버는 사용자 아이디, 디바이스 아이디 그리고 세션키를 확인하는 1단계 인증 과정을 통과한 사용자에 대해 OTA 키 생성에 필요한 홈 서버 공개키를 전송하고, 사용자가 생성한 OTA 키를 확인하는 2단계 인증과정을 수행한다. 이때 생성되는 OTA 키는 홈서버에 접속할 때마다 새로운 OTA 키가 생성되므로 인증키 노출에 대한 보안을 강화시켰고 이중 인증과정을 수행하므로 사용자 아이디 및 디바이스 아이디 노출을 대비하였다. 또한, 단 1회의 인증 연산 횟수를 가지므로 기존의 인증 시스템보다 처리 속도가 빠르며, 별도의 인증키를 사용하므로 데이터 전송량은 많지만 보안측면에 강화시켰다고 볼 수 있다.

Ⅱ. 관련연구

2.1 홈 네트워크 보안기술

홈 네트워크에서는 유무선 네트워크와 다양한 프로토콜 등으로 기존의 인터넷에서 발생하던 보안 취약성외에도 추가적으로 고려해야할 보안 취약성이 많이 존재한다. 더욱이 홈 네트워크에서 디바이스의 다양성과 기기간 자원의 공유 등으로 보안 측면에서 고려해야 할 보안 요구사항이 더욱 복잡해지고 있다[4].

(1) 사용자 인증 : 홈 네트워크에서 각 디바이스를 사용하려는 사람의 신원을 확인하기 위해 사용자 인증이 필요하다. 홈 네트워크에서는 ID/패스워드, 인증서, 스마트 카드, RFID, 생체인식 등 다양한 사용자 인증 기술이 활용되고 있다.

(2) 미들웨어 보안 : 홈 네트워크의 홈 게이트웨이와 각 디바이스를 제어하는 미들웨어에도 보안 기능이 제공되고 있다. 현재 마이크로소프트사 중심의 UPnP(Universal Plug and Play), 썬마이크로시스템사 중심의 Jini, Sony사 중심의 HAVi(Home Audio/Video interoperability) 등이 있다. 표 1은 각 미들웨어 보안을 설명한 것이다[5,6,7,8].

(3) 접근제어 : 홈 구성원별로 제공받을 수 있는 서비스가 다르거나 홈 네트워크 구성요소에 대한 제어 범위가 다를 때, 홈 네트워크에 대한 접근 제어가 요구된다. 홈 네트워크 환경을 고려할 때 접근 제어를 위한 접근제어목록을 단말기에

표 1. 미들웨어 보안 기능
Table 1. Middleware security function

미들웨어	보안기능
UPnP(2.0)	제품인증, 기기간 인증, 접근제어를 위한 디바이스 자체적인 ACL, 기밀성
HAVi	HAVi 인증서를 이용한 인증, 접근제어
Jini	(1.0)사용자 인증, 기기간 인증, 메시지 무결성 및 기밀성, 접근제어 (2.0) 1.0에 추가하여 상호인증, 인가기능, 코드 무결성 기능 강화

내장하고 있는 것이 효율적이라고 할 수 있지만 안전성 측면이나 사용자 측면에서 일관된 보안 정책에 따라 접근 권한이 제어되어야 하므로 홈 게이트웨이에서 종합적으로 관리하는 것이 인증 정보 유출로 인한 불법적인 침입자가 발생할 경우에 능동적으로 대체할 수 있다.

(4) 디바이스 인증 : 홈 네트워크 내에 불법 디바이스 사용을 방지하기 위해 홈 네트워크 구성요소에 대한 디바이스 인증이 필요하다. 현재, 홈 네트워크의 미들웨어에서 디바이스 인증을 제공하고 있다.

(5) 기기간 인증 : 홈 네트워크 서비스를 원활하게 제공하기 위해 홈 네트워크 구성요소간의 자원 공유를 위한 기기간 상호 인증이 필요하다. 현재, 기기간 인증은 미들웨어에서 제공하고 있으나, 다양한 홈서비스를 위한 기본적인 보안 기능이므로 다양한 홈서비스 제공을 위해 기기간 인증 기술이 필요하다.

본 논문에서는 홈 서버가 홈 네트워크를 사용하려는 사용자 인증, 홈 기기에 대한 디바이스 인증, 상호 인증을 제공하도록 설계하였으며, 각각의 인증은 객체화된 모듈로 구성되어 있으므로 홈 서버에 필요한 모듈만 설치하여 사용할 수 있도록 하였다.

2.2 TTAS.KO-12.0030 표준

TTAS.KO-12.0030 표준은 한국정보통신기술협회가 2005년 12월 21일에 제정한 홈 서버 중심의 홈 네트워크 사용자 인증 메커니즘으로 홈 네트워크 서비스 이용자의 안전을 위하여 필요한 댁내 홈서비스 사용을 위한 사용자 인증, 댁내 혹은 댁외 홈 네트워크 사업자가 제공하는 홈 포탈 접근을 위한 사용자 인증, 홈 서버와 홈 네트워크 사업자 인증서버간의 디바이스 인증 메커니즘 등에 대한 표준 규격 기술에 관한 단체 표준이다[9].

(1) 사용자 인증 메커니즘 : 홈 네트워크 서비스를 받고자 하는 사용자는 서비스 이용에 앞서 사용자 인증을 받아야 하고 사용자 인증 메커니즘은 댁내에서 댁내 디바이스를 제어하는 경우, 댁내에서 댁외의 사업자 인증 서버가 제공하는 서비스를 이용하는 경우, 댁외에서 댁내 디바이스를 제어하는 경우의 세 가지로 나누어 고려

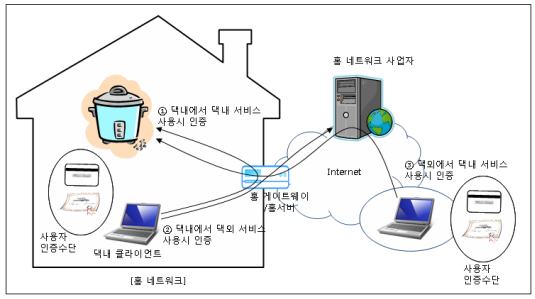

그림 1. 사용자 인증 메커니즘
Fig. 1 User Authentication Mechanism

할 수 있다. 그림 1은 사용자 인증 메커니즘의 세 가지 종류를 설명한 것이다.

댁내에서 댁내 디바이스를 제어하는 홈 네트워크 서비스를 이용할 경우에는 홈 서버가 사용자 인증을 수행하고, 댁내에서 댁외의 사업자 인증 서버가 제공하는 서비스를 이용할 경우에는 사업자 인증 서버가 사용자의 네트워크 접근과 홈 포탈에서 제공하는 사업자 서비스 및 홈서비스 사업자와 계약된 컨텐츠 사업자 서비스 이용에 대한 사용자 인증을 수행한다. 그리고 댁외에서 댁내 디바이스를 제어하는 홈 네트워크 서비스를 이용할 경우에는 사업자 인증 서버가 제공하는 홈 포탈 서비스 이용에 대한 사용자 인증을 사업자 인증서버에서 하고, 사업자 인증서버에서 사용자 인증이 성공적으로 끝나면 사용자 편의성을 위하여 사업자 인증서버에서의 인증정보를 홈 서버에게 전달한다. 네트워크 접근에 대한 사용자 인증은 사업자 인증서버에서 요구할 경우 추가될 수 있다.

(2) 디바이스 인증 메커니즘 : 홈 서버와 사업자 인증서버 사이의 디바이스 인증만을 고려한다. 댁외 디바이스와 홈 서버, 댁내 디바이스와 홈 서버 혹은 사업자 인증서버 사이의 디바이스 인증은 고려하지 않는다.

홈 서버와 사업자 인증서버는 공인인증서 혹은 사설 인증서를 보유해야 하고, 홈 서버와 사업자 인증서버 사이의 인증에는 [RFC 2246] TLS를 적용한다. TLS Handshake 과정의 Cipher_suites 중 anonymous key exchange를 제외한 다른 Cipher_suites를 사용하며, 사업자 인증서버는 항상 client authentication을 요구하여야 한다. 홈 서버는 사업

자 인증서버의 인증이 실패하면 접속을 종료하고, 사업자 인증서버 역시 홈 서버의 인증이 실패하면 접속을 종료하여야 한다.

본 논문에서는 사업자 인증 서버를 배제하므로 사업자 인증서버와 홈 서버간의 디바이스 인증은 필요 없으며, 이미 홈 서버에 등록된 사용자의 기기와 홈 서버간의 디바이스 인증을 하도록 설계하였으므로 인증서가 필요 없다.

Ⅲ. 이중 인증 DA-UDC 모듈 설계

본 논문에서 제안하는 이중 인증 DA-UDC 모듈은 공인 인증서나 사설 인증서를 사용하지 않고, 타원곡선 알고리즘으로 OTA 키를 생성하여 서로의 신분을 상호 인증하거나, 서버가 사용자의 신분을 확인하는 객체형 인증 모듈을 제안한다. 또한, DA-UDC 모듈은 외부에서 사용자가 인터넷망을 통해 홈 네트워크에 접근하며 TTAS.KO-12.0030 표준에서 제안하는 홈 네트워크 사업자는 배제하였다.

3.1 사용자 인증 모듈 설계

인증서버에는 사용자 정보가 등록되어 있다는 가정 하에 그림 3과 같이 사용자가 웹 브라우저를 통해 홈 네트워크 서버에 접속하여 사용자 인증을 요청을 하며 사용자 인증 과정의 각 단계별 설명은 다음과 같다.

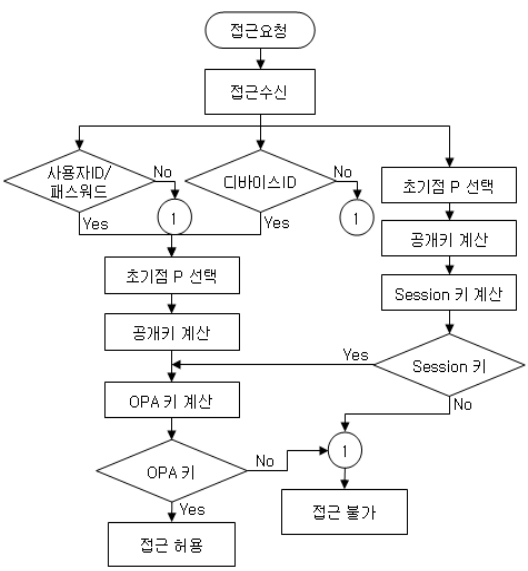

그림 2. DA-UDC 모듈 전체 흐름도
Fig. 2 The Flow of DA-UDC Module

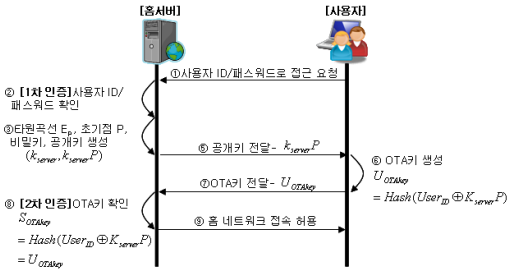

그림 3. 사용자 인증 모듈 흐름도
Fig. 3 The Flow of User Authentication Module

[1 단계] 사용자는 홈 서버에 사용자 ID로 홈 네트워크 접근을 요청한다.

[2 단계] 홈 서버는 사용자 ID가 홈 서버에 등록이 되어 있는지 확인한다. 사용자 ID가 홈 서버에 등록되어 있으면 3단계를 실행하고, 사용자 정보가 등록되어 있지 않으면 홈 네트워크 사용자의 권한이 없다는 메시지를 사용자에게 전달하고 사용자 인증 절차를 종료한다.

[3 단계] 홈 서버는 인증키 생성에 사용될 타원곡선 E_p, 초기점 P, 비밀키 k_{server}를 ECC 알고리즘을 이용해 생성한다. 이때, 홈 서버는 초기점 P를 랜덤하게 선택한다.

[4 단계] 홈 서버는 홈 서버의 공개키 $k_{server}P$를 생성한 후, 홈 서버는 공개키 $k_{server}P$를 사용자에게 전달하는데, 일회용 초기점 P를 이용한 공개키이므로 홈서버 공개키 또한 일회용 공개키가 된다.

[5 단계] 사용자는 홈 서버의 공개키와 자신의 ID를 XOR 연산을 한 후 그 결과 값을 해쉬 연산을 하여 OPA키인 U_{OTAkey}를 생성하여 홈 서버에 전달한다.

$$U_{OTAkey} = Hash\,(User_{ID} \oplus k_{server}P)$$

[6 단계] 홈 서버는 자신의 공개키와 홈 서버에 저장되어 있던 사용자 ID를 XOR 연산을 한 후 해쉬 연산하여 OTA키를 생성한다. 또한, 전달받은 사용자 OTA키 U_{OTAkey}와 서버가 생성한 OTA키인 S_{OTAkey}를 비교한 후 일치하면 사용자를 인증하고 홈 네트워크 접속을 허용한다.

$$S_{OTAkey} = Hash\,(User_{ID} \oplus k_{server}P)$$

그림 4는 사용자 인증 모듈의 알고리즘을 설명한 것이다.

```
DA_UserM_Server(user_id, pwd, u_OTAkey){
  E : 타원곡선
  P : 타원곡선의 일회용 초기점
  k_server : 서버 비밀키
  k_serverP : 일회용 서버 공개키
  u_OTAkey : 사용자 OTA키
  s_OTAkey : 홈서버 OTA키

  switch(step){
   case 1 : if(check_id(user_id, pwd)){
      P= SelectInitPoint(E);
      k_serverP=calculate_server_key(P, k_server);
      send_client(k_serverP);
    } else {
      msg("아이디 혹은 패스워드가 틀렸습니다");
    }
    break;
  case 2 :
      s_OTAkey = Hash(user_id, k_serverP);
      if(s_OTAkey == u_OTAkey)
        msg("접속허용");
      else
        msg("인증키가 틀렸습니다");
    break;
}
```

그림 4. 사용자 인증 모듈 알고리즘
Fig. 4 The Algorithm of User Authentication Module

홈 서버는 사용자가 인증을 요청할 때마다 홈 서버의 공개키를 사용자에게 전달하는데, 이때 사용되는 홈 서버의 공개키는 일회용으로 사용자 ID를 도용해 홈 네트워크의 접속하려는 악의의 사용자의 접근을 통제할 수 있다. 또한, 사용자 인증을 사용자 ID 확인, OPA키 확인으로 두 단계에 걸쳐서 하므로 사용자 ID가 노출되었다고 하더라도 OTA키가 일치하지 않으면 홈 네트워크에 접속할 수 없으므로 홈 네트워크 접속 보안을 한층 강화시켰다고 볼 수 있다.

3.2 디바이스 인증 모듈 설계

홈 네트워크 내에서 디바이스 인증은 사용자를 인증할 때 사용자가 사용하는 홈 기기의 디바이스를 시리얼번호를 이용할 경우와 홈 서버와 홈 네트워크 내의 홈 기기들간의 인증을 할 때 사용한다.

디바이스 인증도 사용자 인증과 마찬가지로 ECC 알고리즘을 이용해 OTA키를 생성하여 인증을 하는데, 사용자 인증과 마찬가지로 네트워크 접속을 요청할 때마다 다른 OTA키를 생성하도록 설계하였다. 즉, 1회용 OTA키를 사용함으로써 OTA키가 노출되

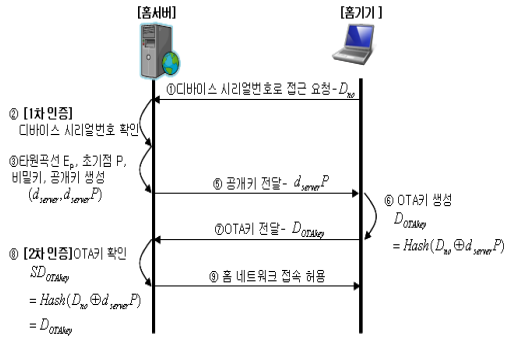

그림 5. 디바이스 인증 모듈 흐름도
Fig. 5 The Flow of Device Authentication Module

더라도 임의의 디바이스로 홈 네트워크에 접근하는 것을 통제할 수 있다.

그림 5는 홈 서버에 새로운 디바이스의 추가와 클라이언트의 사용자 인증 후 디바이스를 직접 제어하기 위한 디바이스 인증 시스템의 인증 과정이다.

디바이스 인증 시스템의 인증과정을 각 단계별 설명은 다음과 같다.

[1 단계] 디바이스가 홈 네트워크 게이트웨이에 접속하면 홈 게이트웨이는 홈 서버에 인증을 요청하게 된다. 이에 홈 서버는 게이트웨이에 디바이스 시리얼 번호를 요청하고, 게이트웨이는 홈 기기에 디바이스 시리얼 번호를 요청한다. 즉, 디바이스는 디바이스 시리얼 번호를 게이트웨이를 통해 홈 서버로 전송함으로써 실질적인 디바이스 인증 요청 과정이 시작된다.

[2 단계] 홈 서버는 디바이스 시리얼 번호가 홈 서버에 등록되어 있는지 확인하고, 등록되어 있으면 다음 단계를 실행하고, 그렇치 않으면 홈 기기가 등록되어 있지 않으므로 홈 기기로 등록 할 것을 공지한다.

[3 단계] 홈 서버는 타원곡선 E_p, 초기점 P, 비밀키 d_{server}를 랜덤하게 생성한다.

[4 단계] 홈 서버는 홈 서버의 공개키 $d_{server}P$를 계산하고, 공개키 $d_{server}P$를 홈 기기에 전송한다.

[5 단계] 디바이스는 자신의 디바이스 시리얼 번호와 홈 서버의 공개키를 XOR 연산을 한 후 그 값은 해쉬 함수로 연산하여 디바이스 OTA키 D_{OTAkey}를 계산한 후, 디바이스 인증키 D_{OTAkey}를 게이트웨이를 통해 홈 서버에 전달한다.

$$D_{OTAkey} = Hash\,(D_{no} \oplus d_{server}P)$$

```
DA_DeviceM_Server(device_id, d_key){
  E : 타원곡선
  P : 타원곡선의 일회용 초기점
  k_server : 서버 비밀키
  k_serverP : 일회용 서버 공개키
  d_OTAkey : 디바이스 OTA키
  sd_OTAkey : 홈서버 OTA키
  switch(step){
   case 1 : if(check_id(device_id)){
      P= SelectInitPoint(E);
      k_serverP=calculate_server_key(P, k_server);
      send_client(k_serverP);
     } else {
       msg("디바이스 ID가 틀렸습니다");
     }
     break;
  case 2 :
       sd_OTAkey = Hash(device_id, k_serverP);
       if(sd_OTAkey == d_OTAkey)
         msg("접속허용");
       else
         msg("인증키가 틀렸습니다");
     break;
}
```

그림 6. 디바이스 인증 모듈 알고리즘
Fig. 6 The Algorithm of Device Authentication Module

[6 단계] 홈 서버는 홈 서버에 등록된 디바이스 시리얼 번호와 홈 서버의 공개키인 $d_{server}P$를 XOR 연산을 하고 해쉬함수로 연산하여 홈 서버용 디바이스 OTA키를 생성한다. 홈 서버는 홈 서버용 디바이스 OTA키 SD_{OTAkey}를 디바이스의 인증키 D_{OTAkey}와 비교하여 디바이스 OTA키를 확인한다.

$$SD_{OTAkey} = Hash\,(D_{no} \oplus d_{server}P)$$

디바이스 인증키가 일치하면 홈 네트워크 내의 홈 기기로 인정을 하여 홈 네트워크 서비스를 제공한다.

그림 6은 디바이스 인증 모듈 알고리즘을 설명한 것이다.

3.3 상호 인증 모듈 설계

홈 서버와 사용자는 필요에 따라서 상호 인증이 필요하다. 사용자가 홈 서버를 인증하고 홈 서버가 사용자의 인증이 필요할 때, 본 논문에서는 사용자 인증과 디바이스 인증을 수행할 때와 마찬가지로 타원곡선 알고리즘을 이용해 동일한 session 키를 생성하고, 생성된 session 키로 OTA키를 다시 한번 생성해 상호 인증을 하도록 설계하였다.

본 논문에서 제안한 상호 인증 기법은 제 1차 상호 인증과 제 2차 상호 인증으로 구성된다. 제 1차 상호 인증에서 session 키가 일치하면 제 2차 상호 인증 단계로 진행하고, 제 1차 상호 인증에서 session 키가 일치하지 않으면 상호 인증에 실패한 것으로 간주한다.

그림 7은 제안하는 상호 인증 시스템의 상호 인증 과정을 설명하는 흐름도로서, 단계별로 살펴보면 다음과 같다.

[1 단계] 사용자가 홈 서버의 신분 인증 요청하거나 홈 서버가 사용자의 신분 인증을 요청할 때, 공개키 계산에 필요한 타원곡선의 초기점 P를 랜덤하게 선택한다.

[2 단계] 사용자는 사용자의 비밀키 K_{user}를 정하고, 초기점 P를 비밀키 K_{user}만큼 Addition 연산을 하여 공개키 $K_{user}P$를 생성한다.

홈 서버 또한 홈서버의 비밀키 K_{server}를 정하고, 초기점 P를 비밀키 K_{server}만큼 Addition 연산을 하여 공개키 $K_{server}P$를 생성한다.

[3 단계] 사용자와 홈 서버는 각자 계산된 공개키 $K_{user}P$, $K_{server}P$를 전달한다.

[4 단계] 사용자는 홈 서버의 공개키 $K_{server}P$를 자신의 비밀키 K_{user}만큼 Addition 연산을 하여 일회용 session 키를 생성한다($S_{user} = K_{user}(K_{server}P)$).

홈 서버 또한 사용자의 공개키 $K_{user}P$를 자신의 비밀키 K_{server}만큼 Addition 연산을 하여 일회용

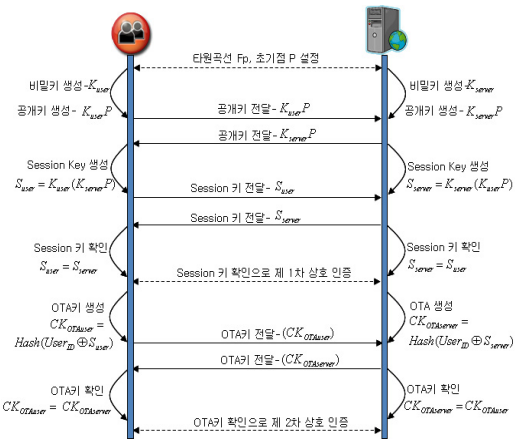

그림 7. 상호 인증 모듈 흐름도
Fig. 7 The Flow of Cross Authentication Module

session 키를 생성한다($S_{server} = K_{server}(K_{user}P)$)

[5 단계] 사용자와 홈 서버는 각자 계산된 일회용 session 키 S_{user}, S_{server}를 전달한다.

[6 단계] 사용자는 사용자의 session 키 S_{user}와 전달받은 홈 서버의 session 키 S_{server}가 같다면, 사용자의 인증키를 생성하고, session 키가 같지 않으면 1차 상호 인증은 실패로 간주한다.

홈 서버 또한 홈 서버 session 키 S_{server}와 전달받은 사용자의 session 키 S_{user}가 같다면, 홈 서버의 인증키를 생성하고, 같지 않다면 제 1차 상호 인증은 실패로 간주한다.

[7 단계] 사용자와 홈 서버는 일회용 session키를 이용해 각자 OTA키 $CK_{OTAuser}$, $CK_{OTAserver}$를 계산하고 상대방에게 전달한다. 단, 홈 서버가 사용하는 사용자 ID는 사용자로부터 전달 받은 ID가 아니고, 홈 네트워크 구성 시 등록된 사용자 ID이다.

$$CK_{OTAuser} = Hash(User_{ID} \oplus K_{user}(K_{server}P))$$
$$CK_{OTAserver} = Hash(User_{ID} \oplus K_{server}(K_{user}P))$$

[8 단계] 사용자는 전달 받은 서버의 인증키 $CK_{OTAserver}$와 사용자가 생성한 인증키 $CK_{OTAuser}$가 동일하다면 사용자가 등록한 홈 서버임을 확인할 수 있고, 동일하지 않다면 사용자가 등록한 홈 서버가 아님을 확인할 수 있다. 홈 서버는 전달 받은 사용자의 OTA키 $CK_{OTAuser}$와 홈 서버가 생성한 OTA키 $CK_{OTAserver}$가 동일하다면 홈 서버에 등록한 사용자임을 확인할 수 있고, 동일하지 않다면 홈 서버에 등록한 사용자가 아님을 확인할 수 있다.

그림 8은 상호 인증 모듈 알고리즘을 설명한 것이다.

본 논문에서 제안한 상호 인증 설계는 Session 키 생성으로 제 1차 상호 인증을 하고, OTA키를 생성하여 비교함으로써 제 2차 상호 인증까지 하도록 하여, session 키가 제 3자에게 노출되더라도 제 2차 상호 인증 단계를 거치면 악의의 사용자 접근을 방지할 수 있다. 또한, 사용자 ID가 노출되더라도 홈 서버가 홈 서버에 저장되어 있던 사용자 ID를 사용하여 인증키를 생성하게 함으로써 상호 인증을 한층 강화시켰다.

```
DA_CrossM_Server(user_pkey, user_skey,
 user_OTAkey){
  E : 타원곡선
  P : 타원곡선의 일회용 초기점
  user_pkey : 사용자 공개키
  user_skey : 사용자 세션키
  server_pkey : 서버 공개키
  k_server : 서버 비밀키
  server_skey : 서버 세션키
  server_OTAkey : 서버 OTA키;
  user_OTAkey : 사용자 OTA키;
  P = SelectInitPoint(E);
  server_pkey = ecc(P, k_server);
  send(server_pkey);
  switch(step){
   case 1 :
     server_skey = ecc(user_pkey, k_server);
     if(user_skey == server_skey){
       send_client(AK_server);
     } else {
       msg("세션키가 틀렸습니다");
     }
     break;
  case 2 :
     server_OTAkey = hash(XOR(user_id,
        server_skey);
     if(server_OTAkey == user_OTAkey)
        msg("접속허용");
      else
        msg("인증키가 틀렸습니다");
    break;
}
```

그림 8. 상호 인증 모듈 알고리즘
Fig. 8 The Algorithm of Cross Authentication Module

Ⅳ. DA-UDC 실험평가

본 논문에서는 제안하는 홈 네트워크의 인증 시스템 구현 환경은 Intel Pentium 4 CPU 2.20, 2GB RAM 그리고 MS-Windows XP Professional 운영체제와 PHP, Javascript, MySQL을 사용하였다.

사용자 ID, 홈기기(디바이스 ID)는 홈 서버에 먼저 등록되어 있다는 가정 하에 실험하였다.

4.1 사용자 인증절차

사용자는 홈서버에 등록된 ID와 Password를 이용해 로그인을 시도하면, 홈 서버는 홈 서버의 공개키를 사용자에게 전송하면, 사용자는 홈서버의 공개키와 사용자 아이디를 이용해 인증키를 생성하여 홈서버에 전달한다. 홈서버는 사용자의 인증키를 확인한 후, 홈 서버에 접속을 허용한다.

그림 9는 타원곡선(F_{23}) $y^2 = x^3 + 12x + 15$일

사용자	홈 서버
아이디/패스워드 (duri/second)	아이디/패스워드 확인 : 1차 인증
	타원곡선(F_{23}) : $y^2 = x^3 + 12x + 15$ 초기점(P)=(5,4) 비밀키(k_{server}) = 4 공개키($k_{server}P$)=4P =(11,11)
인증키 생성(U_{key}) = Hash(duri$\oplus k_{server}P$) =35bc1b07242c41bfe0712c0e6eb784d902a2e824	인증키 생성(S_{key}) = Hash(duri$\oplus k_{server}P$) =35bc1b07242c41bfe0712c0e6eb784d902a2e824
	인증키 확인 : 2차 인증

그림 9. 사용자 인증 절차
Fig. 9 The Process of User Authentication

때, 일회용 초기점을 $P=(5,4)$로 설정한 경우 홈 서버와 사용자간의 동작과정을 설명한 것이다.

4.2 성능평가

표 3은 제안한 DA-UDC 모듈과 기존의 인증 시스템과 성능 분석을 비교한 것이다[4].

기존의 필립스사와 선 마이크로 시스템사는 4회의 사용자 인증 연산횟수를 갖고 마이크로소프트사는 6회의 사용자 인증 연산 횟수를 가지지만, 본 논문에서 제안한 시스템은 단 1회의 사용자 인증 연산 횟수를 가지므로 기존의 시스템보다 사용자 인증 속도가 빠르다. 하지만, 사용자 ID와 서버의 공개키를 이용해 사용자 인증키를 별도로 생성해 사용자 아이디와 연접하여 해쉬한 값을 전송하므로 Data 송신량이 기존의 시스템보다 많지만, 보안적인 면에서는 더 강화되었다.

표 3. DA-UDC 모듈 성능 분석
Table 3. The Performance Analysis of DA-UDC Module

구분	필립스 사	선마이크로 시스템 사	마이크로 소프트 사	제안한 DA-UDC 모듈
사용자 인증시 연산횟수	4회	4회	6회	1회
Hash 연산 횟수	-	-	-	1회
Data 송신량	ID, Key 64+128=192 bit	ID, Key 64+128=192 bit	ID, Key 64+128=192bit	ID, 인증 Key 64+160 =224 bit
암호화 횟수	1회	1회	2회	1회
Key 개수	1개	1개	2개	2개

V. 결 론

홈 네트워크 표준인 TTAS.KO-12.0030이 발표되었지만, TTAS.KO-12.0030은 댁 외에서 홈 네트워크 서비스를 사용하려면 반드시 홈 네트워크 사업자의 서비스에 가입해야 하는 문제점이 있고, 공인인증서를 이용한 사용자 인증 시스템은 공인 인증서의 도용에 따른 문제점이 있다.

본 논문에서는 OTA키를 이용한 일회용 사용자 인증키와 디바이스 인증키를 사용함으로써 공인인증서 도용 문제점을 해결하고, 홈 네트워크 사업자의 서비스에 가입할 필요가 없는 이중 인증 DA-UDC 모듈을 설계하였다. DA-UDC 모듈은 기존의 인증 시스템인 필립스사나 마이크로소프트사의 사용자 인증 횟수인 4회, 6회를 사용자 인증 횟수를 1회로 줄여 사용자 인증 처리 속도가 빠르고, Hash 알고리즘을 이용해 아이디 변조를 방지하여 보안을 좀 더 강화시켰다. 특히, DA-UDC 모듈은 사용자 인증 및 디바이스 인증에서는 홈서버에 등록된 아이디로 1차 인증을 한 후, 홈서버의 일회용 공개키를 이용한 OTA키를 생성하여 제 2차 인증을 하였고, 상호 인증에서는 세션키로 제 1차 상호 인증, OTA키로 제 2차 인증을 하는 이중 인증 모듈로서 사용자 아이디, 디바이스 값, 세션키가 제 3자에게 노출되었다하더라도 제 2차 인증단계에서 악의의 사용자 접근을 방지할 수 있도록 보안을 한층 더 강화시켰다.

참 고 문 헌

〔1〕 Ralph W. Brown, "Home Network Device Authentication", *ITU-T Workshop on Home Networking and Home Service Tokyo*, Japan, 17-18, June, 2004

〔2〕 Carl M.Ellison, "Home Network Security", *Intel Technology Journal*, Vol. 6., No. 4, 2002

〔3〕 Carl M.Ellison, "Interoperable Home Infrastructure Home Network Security", *Intel Technology Journal*, Vol. 6., pp. 37-48, 2002

〔4〕 이영구, *SOAP 기반의 홈 네트워크 구축을 위한*

보안 프로토콜 설계 및 구현, 숭실대학교 대학원, 석사학위, 2006.12.

〔5〕 장영민, 전철용, "홈 네트워크 기술 고찰", *Telecommunications Review*, 제14권 2호, pp.151-163, 2004.

〔6〕 신동일, "홈네트워크 서비스 플랫폼-UPnP 표준기술 분석", *HN FOCUS*, vol. 03, pp48-53, 2005

〔7〕 Jini, http://www.jini.org

〔8〕 Havi, http://www.havi.org

〔9〕 TTAS.KO-12.0030, "홈서버 중심의 홈 네트워크 사용자 인증 메커니즘", *한국정보통신기술협회*, 2005.12.

〔10〕 박중길, 김영진, 김영길, 백규태, 백기영, 류재철, "S/KEY를 개선한 일회용 패스워드 매커니즘 개발" *통신정보보호논문제*, 제9권 제2호, pp28-32, 1999. 6.

정 은 희 (Eun-Hee Jeong) 정회원

1991년 2월 강릉대학교 통계학과 졸업

1998년 2월 관동대학교 전자계산공학과 석사

2003년 2월 관동대학교 전자계산공학과 박사

2003년 9월~현재 강원대학교 삼척캠퍼스 지역경제학과 조교수

<관심분야> 네트워크 보안, 전자상거래, 웹 프로그래밍

이 병 관 (Byung-Kwan Lee) 정회원

1975년 2월 부산대학교 기계설계학과 졸업

1986년 2월 중앙대학교 전자계산공학과 석사

1990년 2월 중앙대학교 전자계산공학과 박사

1988년 3월~현재 관동대학교 컴퓨터학과 교수

<관심분야> 네트워크 보안, 컴퓨터 네트워크, 전자상거래