Journal of Korea Multimedia Society Vol. 16, No. 3, March 2013(pp. 309-317)
http://dx.doi.org/10.9717/kmms.2013.16.3.309

USIM을 활용한 스마트워크 사용자 및 디바이스 인증 기술 연구

위유경[†], 곽 진[††]

요 약

스마트 디바이스의 보급률 증가로 인해 시간과 공간의 제약이 많은 업무 환경을 효율적으로 활용할 수 있는 스마트워크 모바일 이동근무 환경이 발달하게 되었다. 하지만 업무의 효율성을 높여주는 스마트워크 환경에서도 미인증 디바이스에 의한 정보탈취 등 다양한 보안위협이 존재한다. 특히, 다수의 사용자가 접근하는 스마트워크 환경의 특성상 정당한 사용자에 대한 인증과 디바이스 인증에 대한 문제가 크게 대두되고 있는 실정이다. 하지만 이와 같은 스마트워크 환경에 대한 연구가 초기 단계에 머물러 있으며, 그 중에서도 적합한 사용자 인증 기법과 디바이스 인증에 대한 연구가 부족한 실정이다. 따라서 본 논문에서는 스마트워크 환경에서 USIM을 활용한 사용자 및 디바이스 인증 기술에 대해 제안한다.

A Study on USIM Card Based User and Device Authentication Scheme in the Smartwork

Yukyeong Wi[†], Jin Kwak[††]

ABSTRACT

As the distribution rate of smart device increases, users of smartwork are increasingly able to work without constraints imposed by time and space. However, there are many security threats in smartwork environment. Security threats is illegal information for an unauthenticated device. Especially, smartwork environment is approach to users. Therefore, there are other matters concerning justifiable user and device authentication. However, the studies of smartwork are still in early stage of development, and the studies of user and device authentication also not enough to apply smartwork environment. In this paper, we proposed USIM based user and device authentication scheme in the smartwork environment.

Key words: User Authentication(사용자 인증), Device Authentication(디바이스 인증), USIM, Smartwork(스마트워크)

1. 서 론

IT 기술의 혁신적인 발달로 인해 다양한 기술들을 활용한 새로운 방식의 업무 환경인 스마트워크가 주목받고 있다. 특히 스마트워크 환경에서 모바일 디바이스를 활용한 이동근무는 시간과 장소의 제약을 받지 않고 업무를 수행할 수 있도록 도와주는 유연한 근무형태로써 스마트 디바이스의 보급률 증가와 함께 주목받고 있다. 하지만 스마트워크 환경이 다양한 디바이스를 통해 활용되고, 여러 종류의 IT 기술이

※ 교신저자(Corresponding Author) : 곽진, 주소 : 충청남도 아산시 신창면 읍내리 646 순천향대학교 공과대학 정보보호학과(336-745), 전화 : 070) 7516-6293, FAX : 041) 530-4728, E-mail : jkwak@sch.ac.kr
접수일 : 2012년 9월 4일, 수정일 : 2012년 10월 22일
완료일 : 2012년 11월 23일

[†] 준회원, 순천향대학교 정보보호학과 정보보호응용및보증연구실(E-mail : ykwi@sch.ac.kr)
[††] 종신회원, 순천향대학교 정보보호학과
※ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (No. 2012-0003208)

접목되어 있어 기존의 무선네트워크에서 존재하는 취약점과 이동근무에서 새롭게 발생되는 취약점으로 인해 보안 통제가 완벽하게 이루어지기 어렵다. 이러한 보안 취약점이 노출될 경우, 업무와 관련된 중요한 데이터가 유출될 수 있기 때문에 정당한 사용자 인증과 같은 보안 통제가 되지 않는다면 심각한 보안문제가 발생할 수 있다. 만약 사용자가 직접 정당한 사용자 인증 과정을 거쳤다 하더라도 디바이스의 인증이 되지 않는다면 데이터의 무결성을 보장할 수 없다[1,2].

따라서 본 논문에서는 사용자의 모바일 디바이스에서 사용되는 USIM을 활용하여 스마트워크 환경에 적용 가능한 사용자 및 디바이스 인증 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 스마트워크, USIM(Universal Subscriber Identity Module), 사용자 및 디바이스 인증을 위한 기존 연구의 각 방식에 대하여 분석한다. 3장에서는 보안 요구사항에 대해 분석하고, 4장에서는 USIM을 활용하여 스마트워크 환경에 적용 가능한 사용자 및 디바이스 인증 기술을 제안한다. 5장에서는 안전성 및 효율성에 대해 분석하고, 마지막으로 6장에서는 결론을 맺는다.

2. 관련 연구

2.1 스마트워크

스마트워크는 기존에 사무실이라는 한정된 공간에서 업무를 수행하는 개념과는 다르게 시간과 장소의 제약 없이 언제 어디서나 업무를 수행할 수 있는 업무환경으로 스마트폰, 태블릿 PC 등의 모바일 기술, 광대역 통신, 클라우드 컴퓨팅 및 가상화 기술의 발달로 인해 등장하게 되었다[3].

스마트워크 환경은 다양한 디바이스를 통해 구성되고, 여러 종류의 IT 기술이 접목되어 있어 기존에 노출된 취약점과 새롭게 발생되는 취약점으로 인해 보안 통제가 완벽하게 이루어지기 어렵다. 이러한 보안 취약점이 노출될 경우, 업무와 관련된 중요한 데이터가 유출될 수 있기 때문에 정당한 사용자 인증과 같은 보안 통제가 되지 않는다면 많은 경제적 손실을 입을 수 있다. 또한 사용자가 직접 정당한 사용자 인증 과정을 거쳤다 하더라도 디바이스의 인증이 되지 않는다면 데이터의 무결성을 보장 할 수 없다. 이에 따라 스마트워크 환경에서는 정당한 사용자 인증과 디바이스 인증이 필요하다.

2.2 USIM

USIM은 가입자의 ID 정보 등을 탑재한 SIM (Subscriber Identity Module)과 UICC(Universal IC Card)가 결합된 형태로 사용자 인증과 글로벌 로밍, 전자상거래 등의 다양한 기능을 하나의 카드에 구현한 것으로 이동통신 장비에 탑재되어 사용된다. USIM은 소형 CPU와 메모리를 가지고 있어 디바이스의 인증에 사용되는 암호 알고리즘과 프로세스를 작동한다. 또한 네트워크 서비스의 프로필 정보를 메모리에 저장하고 있기 때문에 통신인증 기능 외에도 금융, 신용, 교통카드 등의 기능을 수행할 수 있다.

현재 국내의 각 이동통신사에 미리 USIM 잠금 해제 서비스 등을 신청하게 되면 잠금이 해제된 제 3의 사용자 디바이스에 자신의 USIM을 탑재하여 사용이 가능하다. 단, 같은 이동통신사에 가입한 사용자의 디바이스여야 하며 자신의 디바이스도 잠금이 해제되기 때문에 분실 시에 제 3자가 자신의 단말기를 사용할 수 있는 문제점이 있다. 하지만 W-CDMA 디바이스의 잠금 설정(USIM Lock) 해제를 위한 관련 규정 제정을 의결하여 이동통신사를 바꾸더라도 USIM만 바꿔 탑재하면 이전 디바이스를 그대로 사용할 수 있다. 다만, 이동통신사간 시스템 차이로 인해 전화통화와 SMS만 사용할 수 있다는 제약이 있다[4]. 사용자 데이터의 암호 및 무결성 제공은 단말기가 담당하며, USIM 카드는 인증 과정을 포함하는 키 생성 과정과 사용자 및 디바이스의 인증정보를 저장하게 된다.

2.3 USIM ID 기반 어플리케이션 인증 방식

USIM ID 기반 어플리케이션 인증 방식은 기존의 S/N인증 기법의 온라인 환경이 보장되어야 한다는 인프라 요소적인 단점과 악의적인 침입으로 인하여 인증번호가 공개되거나 어플리케이션이 인증번호를 저장한 채로 복제되어 온라인상에 배포될 수 있는 문제점 때문에 제안되었다. 제안된 방식은 사용자가 인증을 받기위해 USIM ID를 서버에 제공하고, 서버에서는 이를 암호화하여 다시 사용자 기기로 전송한다. 전송받은 사용자 기기는 어플리케이션에 이식하고, 인증을 위해 서버에서 생성한 키와 같은 방식으로 암호화한다. 두 키를 가지고 있는 사용자 기기는

두 키값을 비교하고, 사용자가 어플리케이션을 실행하는 런타임 때마다 서버에서 키를 받은 후 과정을 반복하는 방식이다. 그러나 USIM ID의 길이가 짧고 최초과정에 별도의 암호화과정이 없어 중간자 공격으로 인한 공격자의 ID가 삽입될 경우에 올바른 인증을 수행할 수 없다[5].

2.4 Main/Sub 디바이스 인증/인가 방식

Main/Sub 디바이스 인증/인가 방식은 사내 오피스 네트워크에서 서비스를 제공받던 디바이스가 사외 오피스 네트워크로 이동하였을 때, 사내 오피스 인증 서버로부터 발급받은 인가 티켓을 기반으로 서비스를 지속적으로 제공받을 수 있는 방식이다. 제안된 방식은 오피스 네트워크 환경에서 Main 디바이스가 인증을 요청하고 티켓을 발행받으면 인가 티켓을 기반으로 Sub 디바이스 티켓을 이용하여 오피스 네트워크 서비스를 제공받을 수 있다. 그러나 기존에 발급받은 인증서를 두고 새로운 일회용 인증서를 제차 발급받음으로써 효율성이 떨어질 뿐만 아니라 연산량에도 부담을 주는 단점이 있다[6].

2.5 USIM 기반 모바일 결제 인증 방식

USIM 기반 모바일 결제 인증 방식은 신용카드 정보 노출 및 도용 사고가 끊임없이 일어나고, 소형 PC의 사양으로 진화하는 스마트폰에서 신용카드 결제 시스템의 카드 정보 입력에 대해 유사, 변형적 사고 위험의 우려가 커지는 문제점 때문에 제안되었다. 제안된 방식은 구매자와 카드사 사이에서 직접 통신이 없는 모바일 결제가 가능한 프로토콜을 기반으로 제안되었다. 카드의 다양한 정보를 카드 비밀번호로 대칭키 기반의 암/복호화 시켜 사용하며 또한 암호화된 신용카드 정보는 카드 비밀번호 및 결제정보와 함께 카드 발급 기관의 인증서에 따른 공개키로 암호화되고, 발급 기관의 개인키로 복호화하여 카드의 결제를 인증하는 방식이다. 그러나 신용카드의 결제정보까지 담은 카드 비밀번호의 키 길이가 짧아 안전성이 낮다는 문제점이 있다[7].

3. 보안 요구사항

본 절에서는 앞 절에서 분석한 내용을 바탕으로 스마트워크 환경에서 사용자 및 디바이스 인증의 문제점을 해결하기 위한 보안요구사항을 분석한다[8,9].

3.1 기밀성

서버의 인증 값은 기밀성이 보장되어야 한다. 서버의 인증 값은 사용자 및 디바이스의 ID 생성 정보를 가지고 있기 때문에 공격자에 의해 스마트워크 서버로 접속 가능한 사용자 및 디바이스 ID가 유출될 가능성이 있다. 이를 위해 스마트워크 환경의 통신에 사용되는 데이터는 정당한 사용자만이 확인할 수 있어야 하며, 데이터의 출처 및 수신지, 횟수, 길이 또는 통신선로 상의 트래픽 특성에 대하여 공격자가 알지 못하게 해야 한다[10, 11].

3.2 무결성

디바이스에서 생성되는 랜덤 값은 해당 사용자의 디바이스 ID 생성에 연관이 있기 때문에 무결성이 보장되어야 한다. 스마트워크 환경에서 데이터베이스에 저장 또는 네트워크를 통해 전송되는 데이터가 위변조 및 파괴되지 않도록 해야 한다. 만약에 디바이스 ID의 정보가 유출된다면 위조, 삭제 및 변조를 통해 디바이스 ID 내에 저장되어 있는 서버 인증값을 분석하여 추가적인 보안문제를 야기할 수 있다. 따라서 전송받은 데이터의 위·변조를 감지하기 위해 해쉬함수 연산 및 전자서명 등을 이용해야 한다[12].

3.3 인증

스마트워크 환경에서의 인증기능은 서비스를 이용하고자 접근하는 사용자가 전송한 메시지 또는 데이터의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다[13,14].

3.4 접근제어

정보 자원에 대한 읽기 및 변경 등의 모든 접근 행위에 대해 그 권한을 명백하게 구분하여 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 접근제어 기능이 필요하다. 시스템에서는 운영체제의 접근통제 기능을 사용하며 네트워크에서는 침입차단 시스템을 사용해서 접근통제 수준을 높일 수 있다. 또한 정당하지 않은 사용자는 서비스를 이용할 수 없도록 해야 한다[15,16].

4. 제안 방식

본 논문에서 제안하는 방식은 해당 사용자의 USIM 정보와 디바이스 인증 ID를 USIM의 암호화 모듈에 저장한다. 스마트워크 서버에서는 해당 사용자와 디바이스 리스트를 데이터베이스화하여 인증받지 않은 디바이스로 서버접속을 사전에 차단한다. 또한 향후 서브 디바이스를 확장 또는 추가할 때 USIM 카드만 이동 장착하여 디바이스 인증 ID를 생성하고, USIM 정보와 함께 활용하여 보다 안전하고 편리하게 기업 내부망에 접근하도록 구성하였다. 제안하는 프로토콜은 USIM 발급 과정, 디바이스 등록 과정 그리고 디바이스 확장 과정의 3단계로 이루어진다.

4.1 시스템 파라미터

제안하는 인증 프로토콜에서 사용되는 주요 시스템 파라미터는 다음과 같다.

- $User_x$: 사용자
- Dev_n : 사용자의 n번째 디바이스
- CM : 통신사업자
- DB : 데이터베이스
- $USIM_x$: 사용자 USIM
- ID_x : 사용자의 ID
- PW_x : 사용자의 Password
- SID_x : 사용자의 서버 인증 값
- DID_n : n번째 디바이스의 인증 ID
- SN_{x_n} : 사용자의 n번째 디바이스 시리얼넘버 값
- R_n : 디바이스 n의 랜덤한 값
- t_* : 타임스탬프 값
- $h(\bullet)$: 해쉬함수 연산

4.2 제안 프로토콜

본 논문에서 제안하는 인증 프로토콜의 동작을 세 가지 단계로 구분한다. 기본적으로 디바이스 인증 ID는 디바이스가 USIM 정보를 사용하여 랜덤하게 생성한 값과 해당 디바이스의 S/N 값을 지수승하여 사용한다. 지수승의 모듈러를 이용하는 경우 지수의 값을 알기 어렵기 때문에 높은 안전성을 제공할 수 있다. 먼저, 스마트워크 사용자는 본인 명의의 USIM 카드를 발급받아 사용자 정보를 비교한 후 새로운 USIM 정보를 생성하여 USIM 카드의 암호화 모듈에 저장하고 기업 내부망 서버에 접속하기 위한 USIM 카드와 디바이스를 발급받는 USIM 발급 과정, USIM 카드에 기업 내부망 접속을 위한 디바이스 인증 ID를 생성하는 디바이스 등록 과정, 마지막으로 사전에 등록한 USIM 정보와 디바이스 정보를 기반으로 디바이스를 추가적으로 확장시키는 과정으로

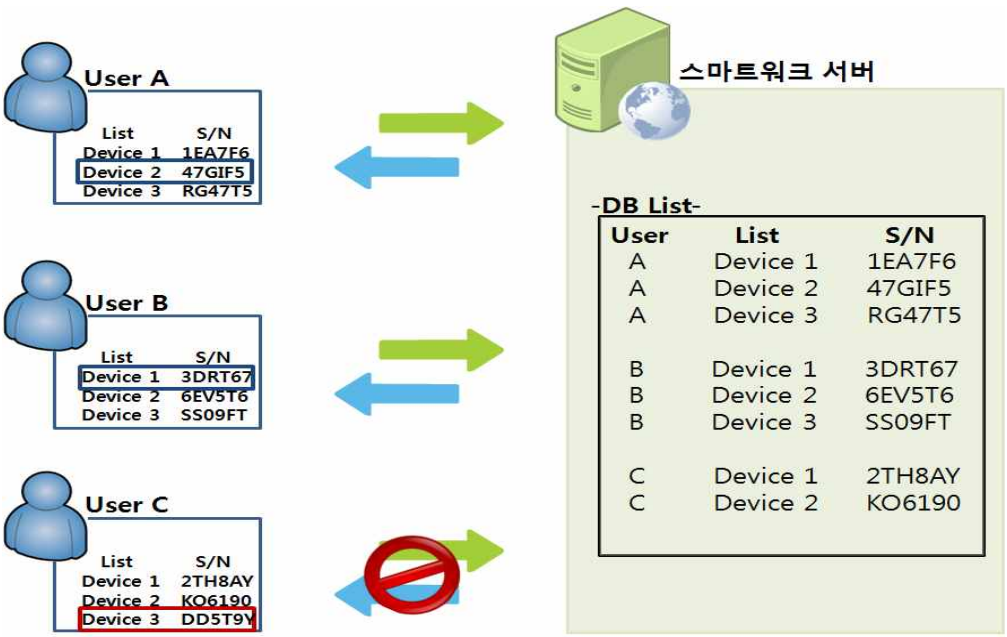

그림 1. 제안하는 사용자 및 디바이스 인증 기술 개요

분류한다.

4.3 USIM 발급 과정

다음의 그림 2는 사용자 본인의 USIM 카드에 기업 내부망 서버 접속을 위한 USIM 정보를 생성한다. 이 정보는 다른 사용자의 부정적인 사용 방지를 위한 USIM 카드에 디바이스를 사전에 등록하는 USIM 발급 과정이다. 사용자는 사용자 본인의 정보를 통신사에 입력하고, 통신사는 통신사 데이터베이스와 비교과정을 수행한다. 확인 후 기업 서버로 사용자 정보를 전송하여 해당 사용자의 서버 인증 값을 발급받는다. 이 후 사용자는 사용하고자 하는 정상적인 디바이스의 S/N 정보를 통신사에 전송하고, 통신사는 전송받은 서버 인증 값과 사용자 정보와 디바이스 S/N 정보를 이용하여 새로운 USIM 정보를 생성하여 USIM 카드를 발급하게 된다. 또한 USIM의 분실 또는 사용불가시에 사전에 입력된 통신사의 입력정보를 통해 해당 사용자의 USIM을 재발급 받을 수 있다.

이 단계는 전송받은 사용자 정보가 사전에 입력되어 있는 정당한 사용자 인지, 또한 해당 디바이스의 S/N 정보를 통해 서비스가 가능한 정상적인 디바이스 인지 확인하는 과정이다. 이 단계는 TLS-SSL이 적용된 안전한 통신망이라 가정한다.

step 1 : 사용자는 해당 통신사에 사용자 정보를 입력한다.
(ID_A, PW_A)

step 2 : 통신사는 자사의 데이터베이스에서 사용자A의 정보와 비교하여 가입여부를 판단한다.
$(CM[DB\,data] = ?\,User_A[ID_A, PW_A])$

step 3 : 통신사는 가입확인이 된 사용자의 정보를 전송하여 회사의 서버로 인증 값을 요청한다.
(ID_A)

step 4 : 서버는 전송받은 사용자의 정보와 서버의 타임스탬프 값을 연산하여 서버 인증 값을 생성하여 통신사에 전송한다.
$(SID_A = ID_A \oplus t_{SV})$

step 5 : 사용자는 가용 디바이스의 S/N를 입력한다.
(Dev_1, SN_{A_1})

step 6 : 통신사는 $Device_1$의 S/N을 데이터베이스와 비교하여 사용가능 여부를 판단한다.
$(CM[DB\,data] = ?\,User_A[Dev_1, SN_{A_1}])$

step 7 : 통신사는 서버로부터 발급받은 서버 인증 값과 입력받은 사용자 정보, 디바이스 정보를 연접하여 USIM 정보를 생성한다.
$(USIM_{A_1} = h(SID_A \parallel ID_A \parallel SN_{A_1}))$

step 8 : 사용자에게 USIM 카드를 발급함으로써 과정을 마무리한다.

4.4 디바이스 등록 과정

다음의 그림 3는 사용자 본인의 USIM 카드에 기업 내부망 서버 접속을 위한 DID_n를 생성하여 디바이스를 등록하는 과정이다. 사용자는 사용자 $USIM_x$ 정보가 저장된 USIM 카드를 사전에 등록 과정이 완

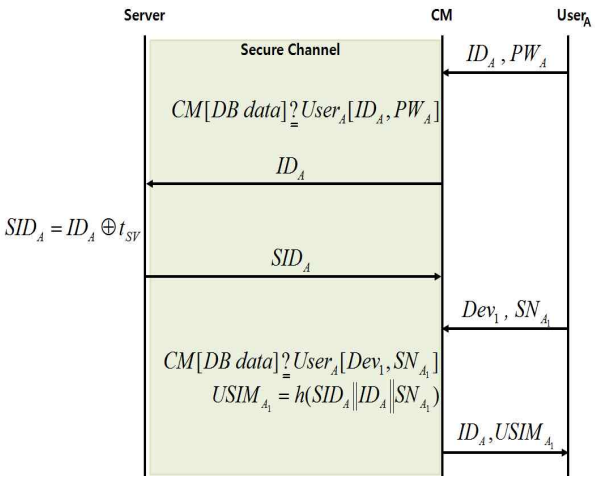

그림 2. USIM 발급 과정

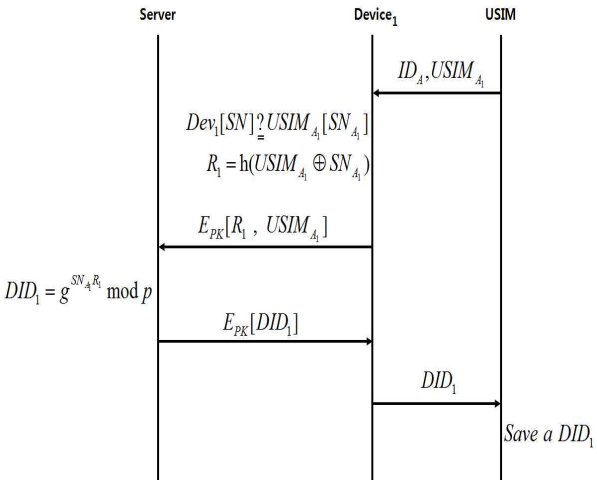

그림 3. 디바이스 등록 과정

료된 디바이스에 장착한다. 디바이스는 사용자 $USIM_x$ 정보의 S/N 정보와 자신의 S/N 정보를 비교하여 등록 여부를 판단한다. 일치할 경우 전송받은 USIM 정보와 S/N 정보를 연산하여 디바이스 인증 ID (DID_n) 생성에 필요한 랜덤 값($R_1 = h(USIM_{A_1} \oplus SN_{A_1})$)을 생성하여 암호화하여 서버에 전송하게 된다. 그 후 디바이스로부터 전송받은 랜덤 값을 기반으로 디바이스 인증 ID(DID_n)를 생성하여, USIM 카드의 암호화모듈에 저장하는 과정은 다음과 같다.

step 1 : $Device_1$에 USIM 카드를 장착하여 $USIM_{A_1}$의 정보를 전송한다.
(ID_A, $USIM_{A_1}$)

step 2: $USIM_{A_1}$의 S/N정보와 $Device_1$의 S/N 정보를 비교한다. 불일치할 경우 더 이상 등록이 수행되지 않는다.
($Dev_1[SN] = ? USIM_{A_1}[SN_{A_1}]$)

step 3 : $Device_1$은 S/N정보가 일치한다면 랜덤 값을 생성하여 회사의 서버로 전송한다.
($R_1 = h(USIM_{A_1} \oplus SN_{A_1})$)

step 4 : 서버는 전송받은 랜덤 값과 $USIM_{A_1}$의 정보를 이용하여 $Device_1$의 인증 ID를(DID_*) 생성한 후 디바이스로 전송한다.
($DID_1 = g^{SN_{A_1} R_1} \bmod p$)

step 5 : 디바이스는 전송받은 자신의 DID_*를 내부 메모리와 USIM 카드에 각각 저장하여 등록 단계를 마무리 한다.

4.5 디바이스 확장 과정

다음의 그림 4는 디바이스를 확장하는 과정이다. 사용자는 확장하고자 하는 디바이스의 S/N 정보를 앞서 사용하고 있던 1번 디바이스($Device_1$)를 통해 통신사에 S/N 정보를 입력하게 된다. 이 과정을 통해 사전에 등록된 디바이스 없이는 추가적인 디바이스의 확장 또한 불가능하게 되며, 부정한 디바이스 역시 등록이 불가능하게 된다. 디바이스를 확장하는 과정은 다음과 같다.

step 1 : 사용자는 $Device_1$을 사용하여 통신사에 $Device_2$의 S/N정보를 입력하여 등록을 요청한다.
(ID_A, Dev_2, SN_{A_2})

step 2 : 통신사는 자사의 데이터베이스에서 $Device_2$의 등록여부를 비교한다. 만약 이미 등록된 기기 또는 정상적인 기기가 아니라면 등록이 더 이상 불가하다.
($CM[DB\,data] = ? User_A[Dev_2, SN_{A_2}]$)

step 3 : 통신사는 서버로 $User_A$의 서버 인증 값을 요청한다.
(ID_A)

step 4 : 서버는 전송받은 사용자의 정보와 서버의 타임스탬프 값을 연산하여 서버 인증 값을 생성하

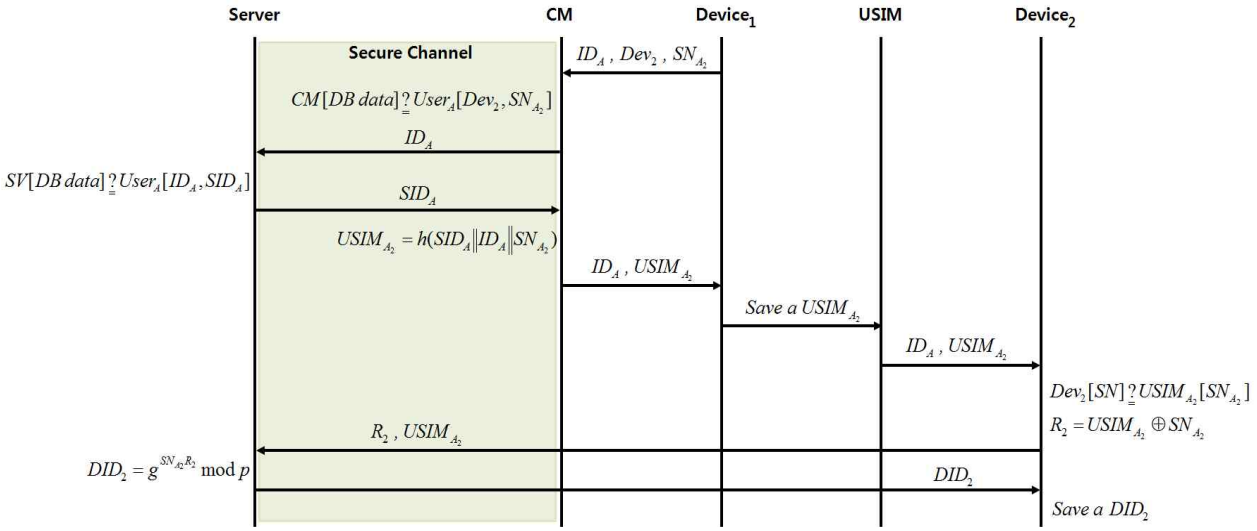

그림 4. 디바이스 확장 과정

여 통신사에 전송한다.
($SID_A = ID_A \oplus t_{SV}$)

step 5 : 통신사는 서버로부터 발급받은 서버 인증 값과 입력받은 사용자 정보, 디바이스 정보를 연접하여 $USIM_{A_2}$ 정보를 생성하여 $Device_1$로 발급한다.
($USIM_{A_2} = h(SID_A \| ID_A \| SN_{A_2})$)

step 6 : USIM 카드에 $USIM_{A_2}$를 저장한 후에 USIM 카드를 $Device_1$에서 해제한다.

step 7 : USIM 카드를 $Device_2$에 장착하여 $USIM_{A_2}$의 SN_{A_2} 정보와 $Device_2$의 S/N 정보를 비교한다. 불일치할 경우 더 이상 등록이 수행되지 않는다.
($Dev_2[SN] = ? USIM_{A_2}[SN_{A_2}]$)

step 8 : $Device_2$은 S/N정보가 일치한다면 랜덤 값을 생성하여 서버로 전송한다.
($R_2 = USIM_{A_2} \oplus SN_{A_2}$)

step 9 : 서버는 전송받은 랜덤 값과 $USIM_{A_2}$의 정보를 이용하여 $Device_2$의 인증 ID를 생성한 후 디바이스로 전송한다.
($DID_2 = g^{SN_{A_2} R_2} \bmod p$)

step 10 : 디바이스는 전송받은 자신의 디바이스 ID(DID_2)를 내부 메모리와 USIM 카드에 각각 저장하여 디바이스 확장 단계를 마무리 한다.

5. 안전성 및 효율성 분석

본 장에서는 제안 방식의 프로토콜의 안전성과 효율성 분석을 앞에 제시한 3장의 보안 요구사항에 따라 분석한다.

5.1 안전성 분석

■ 기밀성

서버의 인증 값은 사용자 및 디바이스의 ID 생성 정보를 가지고 있기 때문에 기밀성이 보장되어야 한다. 본 논문에서 제안하는 사용자 및 디바이스 인증 기법은 디바이스의 랜덤한 값과 S/N를 지수승하여 디바이스 인증 ID를($DID_1 = g^{SN_{A_1} R_1} \bmod p$) 생성한다. 따라서 해당되는 지수의 값을 알기 어렵기 때문에 해당 디바이스 인증 ID를 탈취하더라도 디바이스를 사용할 수가 없다. 또한 USIM을 별도로 탈취하게 되더라도 인증된 디바이스에서만 사용이 가능하도록 USIM 정보($USIM_{A_1} = h(SID_A \| ID_A \| SN_{A_1})$)를 사용하므로 해당 사용자 이외에 USIM 카드를 사용할 수가 없다.

■ 무결성

사용자 및 디바이스 랜덤값은 해당 사용자의 디바이스 ID 생성에 연관이 있기 때문에 무결성이 보장되어야 한다. 본 논문에서 제안하는 사용자 및 디바이스 인증 기법은 해쉬함수를 사용하여 USIM 정보를 해쉬값을 통해 생성하여 USIM 카드에 저장하게 된다($USIM_{A_1} = h(SID_A \| ID_A \| SN_{A_1})$). 생성된 USIM 정보는 디바이스의 등록과정에서 S/N 정보와의 비교를 통해 등록 가능한 디바이스인지 여부를 판별하므로 무결성을 제공한다.

■ 인증

본 논문에서 제안하는 사용자 및 디바이스 인증 기법에서 디바이스 인증 ID(DID_1)는 USIM 정보와 디바이스의 랜덤한 값을 지수승 연산을 통해 생성되므로 지수의 값을 알기 어렵기 때문에 안전한 인증기능을 제공한다($DID_1 = g^{SN_{A_1} R_1} \bmod p$). 또한 USIM 카드에 저장된 USIM 정보를 활용하여 해당 사용자의 제 2, 3의 디바이스에 장착시 디바이스 인증 ID만 새롭게 부여받게 되어 기존기법들에 비해 높은 효율성을 제공한다
($DID_1 = g^{SN_{A_1} R_1} \bmod p, DID_2 = g^{SN_{A_2} R_2} \bmod p$).

■ 접근제어

제안하는 사용자 및 디바이스 인증 기법은 통신사업자로부터 발급받은 USIM 정보의 값이 없다면 접근이 불가능하다. 또한 디바이스 인증 ID를 통해 서버로 정상적인 접근이 가능한 디바이스인지 여부를 판단 받게 된다. 디바이스 인증 ID는 USIM 정보와 디바이스로부터 랜덤 값을 사용하여 생성하므로 이를 알아내기는 어렵다. 그러므로 불법적인 사용자는 스마트워크 서버의 DB에 접근할 수 없어야 한다. 또한 해당 디바이스의 불법적인 사용과 불법 사용자로부터 디바이스 조작을 방지할 수 있다.

5.2 효율성 분석

■ 통신 회수에 따른 효율성

제안하는 사용자 및 디바이스 인증 기법의 총 통신 회수는 USIM 발급 과정, 디바이스 등록 과정, 디

표 1. 제안 방식과 기존 시스템의 안전성 및 효율성 분석

	기존방식 1 [5]	기존방식 2 [6]	기존방식 3 [7]	제안방식
기밀성	X	○	X	○
무결성	○	○	X	○
사용자 인증	○	X	○	○
디바이스 인증	X	○	X	○
접근제어	○	○	○	○
해쉬함수 연산	1회	3회	X	2회
총 통신 회수	12회	13회	19회	10회
인증 회수	4회	4회	5회	5회

[○: 안전, X: 안전하지 않음]

바이스 확장 과정까지의 모든 단계를 포함한 것이므로 기존 방식의 인증 단계만의 회수와 비교할 때 높은 효율성을 제공한다 할 수 있다. 또한 총 통신회수의 감소로 인해 프로토콜의 처리속도가 기존방식에 비해 개선되었다.

6. 결 론

스마트워크는 스마트 기기와 통신 인프라를 기반으로 하는 혁신적인 IT 서비스의 대표적인 기술이다. 기업은 생산성 향상과 편리성 증대를 위해 많은 비용과 노력을 투입하여 스마트워크를 환경을 구축하고 있다. 그러나 디바이스의 분실, 모바일 악성코드의 감염, 기업정보 및 기밀의 무단 유출과 같은 보안 문제가 지적되고 있다. 또한 유·무선 디바이스를 이용하여 기업 외부에서 기업 내부로 네트워크를 통해 접근을 수행하게 되는 스마트워크 환경에서는 사용자에 대한 정당한 인증 과정과 정당한 디바이스의 인증 과정이 요구된다. 이러한 보안 문제에 대한 개선 없이는 안전한 스마트워크 환경을 구축할 수 없다.

본 논문에서는 스마트워크 환경에 접근하는 다양한 사용자에 대해 USIM 카드를 활용한 사용자 및 디바이스 인증 기술을 제안하였다.

이를 통해 스마트워크 환경을 구축하고 기업 내부망에 접근하여 업무를 수행할 때 사용자 고유의 USIM 정보와 디바이스 인증 ID를 사용하기 때문에 인증되지 않은 사용자에 대한 원천적 차단이 가능하고, 중요한 데이터의 노출에 대한 차단이 가능할 것으로 기대할 수 있다. 또한 USIM의 활용하여 편리하게 제 2, 3의 디바이스를 확장 시킬 수 있다. 따라서 스마트워크 모바일 환경의 전반에 대한 보안성과 편의성을 향상시킬 수 있을 것으로 기대된다.

참 고 문 헌

[1] 위유경, 곽진, “스마트워크 환경에서 음성인식을 활용한 사용자 인증 기법에 관한 연구,” 한국지식정보기술학회 논문지, 제6권, 제6호, pp. 23- 31, 2011.

[2] 신유진, 장현미, 김경진, 양새로미, 이연우, 홍승필, “멀티 디바이스 환경 내 통합 사용자 인증 설계 방안,” 한국인터넷정보학화 추계학술대회 논문집, 제12권, 제2호, pp. 95-96, 2011.

[3] 방송통신위원회, “스마트워크 활성화 추진계획,” 2011.

[4] 김두환, 정수환, “3GPP 네트워크에서 효율적인 인증 데이터 관리를 위한 개선된 AKA 프로토콜,” 한국정보보호학회 논문지, 제19권, 제2호, pp. 93-103, 2009.

[5] 김성제, 조용환, 이태우, “모바일 환경에서 USIM ID를 이용한 어플리케이션 인증 기법,” 한국엔터테인먼트산업학회 추계학술대회 논문집, pp. 99-106, 2011.

[6] 문종식, 이임영, “유비쿼터스 오피스 네트워크에서의 Main/Sub 디바이스 인증/인가 프로토콜,” 한국정보보호학회 논문지, 제19권, 제 5호, pp. 105-118, 2009.

[7] 지은희, 김애영, 이상호, “USIM 탑재 스마트폰 기반 모바일 신용카드 결제 프로토콜의 안전성 향상,” 한국정보과학회 논문지, 제17권, 제4호,

pp. 259-263, 2011

[8] Jongsik Moon and Imyeong Lee, “Authentication Protocol Using an Identifier in an ad Hoc Network Environment,” Mathematical and Computer Modelling, Vol 55, No. 1-2, pp. 134-141, 2012.

[9] 문종식, 한승완, 이임영, “모바일 클라우드 컴퓨팅 환경의 스마트 디바이스용 일회용 인증서 기반 권한 관리 기술,” 한국정보처리학회 춘계학술대회 논문집, 제18권, 제1호, pp. 832-835, 2011.

[10] 유형준, 박중길, 고재영, 하경주, “무선 네트워크 환경에서 디바이스 신뢰성 보장을 위한 인증 방안,” 한국정보과학회 논문지, 제39권, 제3호, pp. 239-247, 2012.

[11] 강서일, 이남훈, 이임영, “Ad-hoc 네트워크에서 모바일 디바이스 아이디 기반의 그룹 키 관리에 대한 연구,” 한국멀티미디어학회 논문지, 제12권, 제4호, pp. 540-549, 2009.

[12] 박대식, 곽진, “안전성이 향상된 스마트카드 기반 원격 사용자 인증 프로토콜,” 한국지식정보기술학회 논문지, 제6권, 제4호, pp. 27-34, 2011.

[13] 이정환, 황유동, 박동규, 한종욱, “홈 네트워크 환경에서 신뢰할 수 있는 서비스를 위한 디바이스 인증 프로토콜,” 한국정보기술학회 논문지, 제3권, 제6호, 2005.

[14] 이윤석, 김은, 유현주, 정민수, “스마트 카드를 사용한 멀티 서버환경에서의 사용자 인증 기법,” 한국멀티미디어학회 학술발표논문집, pp. 50-53, 2010.

[15] 강명희, 유황빈, “유비쿼터스 컴퓨팅 환경에서의 익명성을 보장하는 사용자 인증 및 키 동의 프로토콜 설계,” 한국정보보호학회 논문지, 제16권, 제2호, pp. 3-12, 2006.

[16] 김은, 이윤석, 정민수, “스마트카드를 이용한 위조방지 인증 시스템 설계 및 구현,” 한국멀티미디어학회 논문지, 제14권, 제2호, pp. 249-257, 2011.

위 유 경

2006년 3월~2012년 2월 순천향대학교 정보보호학과 학사

2012년 3월~현재 순천향대학교 정보보호학과 석사과정

관심분야 : 정보보호제품평가, 스마트워크 보안, 제어시스템 보안

곽 진

성균관대학교 학사, 석사, 박사

2006년 4월~2006년 일본 큐슈대학교 시스템정보공학부 방문연구원

2006년 8월~2006년 11월 일본 큐슈시스템정보기술연구소 특별연구원

2006년~2007년 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관

2007년 3월~현재 순천향대학교 정보보호학과 교수

관심분야 : 암호프로토콜, 응용시스템 보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 보안 등