Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1551

원격 건강정보 모니터링 시스템을 위한 개선된 익명인증 기법*

박 영 호,† 노 시 완, 이 경 현‡
부경대학교

An Improved Anonymous Authentication Scheme for Remote Health Monitoring System*

Youngho Park,† Si-Wan Noh, Kyung-Hyune Rhee‡
Pukyong National University

요 약

스마트 헬스케어 기술의 발전과 웨어러블 디바이스의 증가로 인해 최근 WBN을 활용한 원격지 건강정보 모니터링 시스템이 제시되고 있다. 그러나 네트워크를 통해 전송되는 환자 개인의 건강기록에 대한 보호가 필요하며, 허가되지 않은 정보의 수집으로 인한 환자의 개인 식별정보나 건강기록이 노출되지 않도록 환자의 프라이버시도 반드시 보호되어야 한다. 이를 위해 Yang 등은 암호기술의 키 격리 기법을 적용한 원격 건강정보 모니터링 시스템의 익명 인증기법을 제안하였다. 그러나 이들의 기법은 키 격리 기법을 잘못 구성하여 다른 사용자의 개인키 위조 가능성 문제를 가지고 있으며, 헬스케어 서비스 제공자에게 사용자의 식별정보가 그대로 노출되어 익명성을 보장하지 못한다. 이에 본 논문은 Yang 등의 기법의 보안상의 문제점을 지적하고, 이를 개선한 건강정보 모니터링 시스템의 익명인증 기법을 제안한다.

ABSTRACT

With the advancement of wearable devices and wireless body are networks, smart healthcare systems based on such technologies have been emerging to effectively monitor patient health and disease progression. In order to implement viable smart healthcare systems, the security and privacy of patient's personal health information must be considered. Yang et al. proposed a privacy-preserving authentication scheme using key-insulation technique for remote health monitoring system, however, key-insulation technique is not properly adapted to their scheme which in turn causes a security pitfall contrary to their assertions. Besides, Yang et al.'s scheme does not guarantee user anonymity against healthcare service provider. Therefore, in this paper, we discuss the security concerns for Yang et al.'s scheme and present an improved anonymous authentication scheme.
Keywords: Remote Healthcare, Authentication, Anonymity, Key-insulation

I. 서 론

고령 인구의 증가와 건강하고 편안한 삶에 대한 욕구 증대로 스마트 헬스케어 기술이 많은 관심을 받고 있다. 또한 WBANs(Wireless Body Area Networks)과 결합하여 원격지 환자의 건강상태를 효과적으로 수집하고 모니터링하기 위한 서비스도 최근 주목받고 있다. 휴대형 단말이나, 센서, 웨어러블

Received(05. 03. 2016), Modified(1st: 08. 30. 2016, 2nd: 11. 03. 2016), Accepted(11. 03. 2016)
* 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2014R1A2A1A11052981).
* 본 논문은 2016년도 영남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, pyhoya@pknu.ac.kr
‡ 교신저자, khrhee@pknu.ac.kr(Corresponding author)

(wearable) 디바이스들을 통해 사용자 혹은 환자의 생리학적 정보를 수집하고, 이를 의료진들로 구성되는 헬스케어 서비스 제공자에게 인터넷을 통해 전달함으로써 효율적으로 환자의 건강기록을 관리하고 진단하기 위함이다.

IEEE802.15.6 WBAN 기술은 저전력 무선 센서 노드를 위한 근접 통신기술 표준으로서, 병원이나 홈네트워크 환경에서 개인 혹은 환자의 생체 의학적(biomedical) 정보를 수집하는 응용에 널리 이용되고 있다. 무선 의료센서 노드들을 통해 수집된 개인의 생체의학 정보들을 헬스 모니터링 시스템으로 전송함으로써 의료진이 원격지에서 환자의 건강상태 검사나 진단을 가능하게 한다. 그러나 실용적인 원격 의료서비스를 구축하기 위해서는 네트워크를 통해 전송되는 개인 생체의료정보에 대한 보호와 사용자/환자의 익명성이 보장되어야 한다.

원격 의료 서비스 제공을 위한 TMIS(Telecare Medical Information System)는 센서를 통해 측정된 데이터가 헬스케어 서버에 저장되고, 데이터 분석을 통해 환자별 맞춤 서비스를 제공하는 시스템이다. 원격의료시스템의 익명 인증 기법에 대한 연구는 대부분 TMIS의 사용자 로그인에 초점을 맞추어 주로 연구되고 있다[1-4]. 이들의 연구는 TMIS 사용자 로그인을 위해 스마트카드와 패스워드 인증을 결합하고, 도청으로부터 사용자 식별정보를 보호하기 위한 방안을 제안하였다. 하지만 [1-4]에서 제안된 기법들은 안전성에 문제가 발견되고 초기기법의 보안 문제를 단순 개선하는 형태로 제안되었으며, 시스템으로 전송되는 사용자 개인 건강정보의 익명성 보장에 대해서는 고려하지 않았다.

사용자의 식별정보에 대한 익명성뿐만 아니라 네트워크를 통해 전송되는 환자 개인의 건강정보(Personal Health Information, PHI)에 대한 보호도 필요하며, 허가되지 않은 PHI의 수집으로 인한 환자의 개인 식별정보나 건강기록이 노출되지 않도록 환자의 프라이버시도 반드시 보호되어야 한다[5-8]. Lin 등은 스마트폰과 무선 헬스케어 시스템을 이용한 원격지 환자 건강상태 모니터링 서비스 환경에서 전역적 도청 공격으로부터 환자의 건강기록과 식별정보를 보호하기 위한 프라이버시 보호 헬스케어 프로토콜을 제안하였다[5]. 익명 인증을 위해 Lin 등은 환자의 가명 식별자와 신원기반 암호기술(Identity-based cryptography)[9,10]을 결합하여 환자의 익명성을 보장하면서 전송 PHI를 보호하기 위한 시스템을 구성하였다.

Yang 등은 환자의 PHI 전송 보안 프로토콜을 처리하는 스마트폰의 도난이나 분실로 인해 스마트폰에 저장된 개인키가 손상될 우려가 있음을 제기하고, 신원기반 암호의 키 격리(Key-insulation) 기법을 적용한 익명 인증기법을 제안하였다[8]. 키 격리 기법은 사용자의 개인키는 안전한 보관소에 저장하고, 개인키로부터 생성된 짧은 시간주기의 임시 개인키를 스마트폰과 같은 휴대용 단말기에 저장하여 사용함으로써, 단말기 분실로 인한 개인키 노출의 피해를 최소화하기 위한 기법이다[11-13]. 그러나 Yang 등은 익명인증 시스템을 설계함에 있어서 키 격리 기법을 잘못 구성하여 단말기 분실 시 타 사용자의 개인키 위조 문제가 발생할 수 있으며, 헬스케어 서버에게 환자의 실제 식별정보가 그대로 제공되어 익명성을 보장하지 못하는 문제를 가지고 있다.

이에 본 논문에서는 [8]에서 Yang 등이 제안한 원격 건강정보 모니터링 시스템의 익명인증 기법의 보안상 문제점을 지적하고, 이를 개선한 익명인증 기법을 제안한다. 본 논문의 구성은 다음과 같다. Ⅱ장에서는 Yang 등의 기법에 대해 고찰하고, Ⅲ장에서는 제안하는 시스템 모델 및 익명 인증기법에 대해서 기술하며, Ⅳ장에서 제안기법에 대한 분석과 개선 결과를 비교하고, 마지막으로 Ⅴ장에서 결론을 맺는다.

II. Yang 등의 기법 고찰

본 장에서는 Yang 등이 제안한 신원기반 키 격리 기법을 이용한 헬스케어 모니터링 시스템 익명 인증 프로토콜을 소개하고 Yang 등의 기법의 문제점을 살펴본다.

2.1 시스템 구성

Yang 등은 헬스케어 모니터링 서비스의 익명 인증을 위해 Fig. 1과 같은 시스템 모델을 제시하였으며, 각 개체의 역할은 다음과 같다.

- HMS (Health Monitoring Server)
  환자의 가명 및 참여 개체들의 키 발급을 담당하는 개체로서, 의사와 환자 간의 건강정보 전달 중개자 역할을 한다.
- 환자 (Patient)
  헬스케어 서비스 대상자로서 자신의 건강정보를 제공하고 그에 대한 의사의 진단을 요청한다.

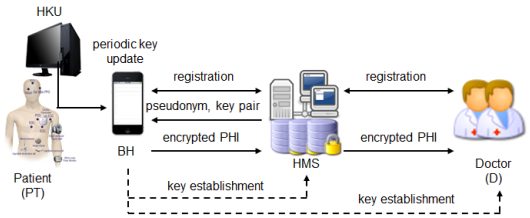

Fig. 1. System model of Yang et al.'s.

- 의사 (Doctor)
  환자의 건강정보에 대해 진단을 하는 개체로서, 의사들은 HMS에 소속되어 있다.
- BH (Body Hub)
  센서들을 통해 측정된 환자의 건강정보를 HMS로 전달하는 장치로서 일반적으로 개인이 소유한 스마트폰을 가정한다.
- HKU (Helper of Key Update)
  BH에서 사용할 짧은 주기의 개인키 생성을 보조하는 장치로서, 사용자 개인 PC 등이 HKU 기능을 수행할 수 있다.

2.2 키 격리 기법을 이용한 헬스케어 인증

Yang 등이 제안한 익명 인증 기법은 다음과 같이 구성된다.

1) 시스템 초기화

시스템 초기화 단계에서 HMS는 신원기반 암호를 위한 겹선형 그룹[9] 파라미터 $(G, G_T, q, P, \hat{e})$를 생성하고, HMS의 비밀키 $s, h_1 \in Z_q^*$를 선택한 후 $P_{pub} = sP$와 $P_{HMS} = hP$를 각각 계산한다. 이때, s는 신원기반 키 발급을 위한 비밀키이고 h는 키 격리 기법을 위한 HKU의 헬퍼 비밀키(helper secret key)로 사용된다. 이후 HMS는 공개 시스템 파라미터 $\langle G, G_T, q, P, \hat{e}, P_{pub}, P_{HMS}, H_1 \rangle$를 배포한다. 여기서 $H_1 : \{0,1\}^* \rightarrow G$는 일방향 해시함수이다. 일부 표기는 Table 1에 나타낸 표기와 의미를 같이 한다.

2) 등록 및 키 발급

시스템에 등록되는 환자 PT_i에 대해, HMS는 환자의 초기 개인키 $PSK_i^0 = sH_1(PT_i) + hH_1(PT_i|0)$를 계산하여 헬퍼 비밀키 h와 함께 환자에게 안전하게 전달한다. 이때 h는 HKU에 안전하게 저장된다. 또한 시스템에 등록되는 소속 의사 DT_j에 대해 신원기반 개인키 $SK_j = sH_1(DT_j)$를 발급한다.

3) 키 갱신

환자 PT_i는 시스템의 t번째 주기가 시작되는 시점에 자신의 t-주기 개인키 PSK_i^t를 갱신한다. 먼저 HKU를 통해 t-주기 임시 헬퍼키 $TK_i^t = h(H_1(PT_i|t) - H_1(PT_i|t-1))$를 획득하고, BH에서 t-주기 개인키 $PSK_i^t = PSK_i^{t-1} + TK_i^t$를 생성한다.

4) 건강기록 전송

환자는 자신의 건강기록을 HMS에게 안전하게 전송하기 위해 현재 t-주기의 개인키를 이용하여 신원기반 암호기법의 비대화식(non-interactive) 키 설정기법을 통해[10,14] HMS와 공유하게 될 비밀키 $K_{PT_i - HMS} = \hat{e}(PSK_i^t, H_1(HMS))$를 설정한다. 이때, HMS는 $K_{PT_i - HMS} = \hat{e}(H_1(PT_i), sH_1(HMS))\,\hat{e}(H_1(PT_i), P_{HMS})$와 같이 공유 비밀키를 계산할 수 있다. 이후로 HMS는 $K_{PT_i - HMS}$를 이용하여 PT_i를 인증하고, 환자에게 지정된 의사 DT_j와 건강기록 전송 프로토콜 수행에 필요한 환자의 가명 pid_i와 가명에 대한 개인키 $SK_{pid_i} = sH_1(pid_i)$를 발급한다. 이후 환자는 가명 기반 개인키를 이용하여 의사와 공유할 비밀키 $K_{pid_i - DT_j} = \hat{e}(SK_{pid_i}, H_1(DT_j))$를 설정할 수 있으며, 세부적인 프로토콜 설명은 생략한다.

2.3 고찰

1) 단일 헬퍼 비밀키 문제

Yang 등은 키 격리 기법을 위한 단일 헬퍼 비밀키 h를 생성하고 이에 대한 공개키 $P_{HMS} = hP$를 HMS의 공개 시스템 파라미터에 포함하여 배포하고 있다. 그러나 Yang 등은 헬퍼 비밀키를 보관하기 위한 HKU의 역할을 사용자 개인용 스테이션이 수행할 수 있다고 가정하고 있으며, 시스템에 등록된 누군가가 다른 사용자의 BH를 습득한 경우 $t+1$ 주기의 개인키를 위조할 수 있는 문제점을 가진다. 예를 들어, 사용자 PT_j가 PT_i의 t주기 개인키 $PSK_i^t = sH_1(PT_i) + hH_1(PT_i|t)$를 습득한 경우,

PT_j 자신의 HKU에 저장된 h를 이용하여 $TK_i^{t+1}=h(H_1(PT_i|t+1)-H_1(PT_i|t))$를 계산하고 $PSK_i^{t+1}=PSK_i^t+TK_i^{t+1}=sH_1(PT_i)+hH_1(PT_i|t+1)$를 생성할 수 있으므로 PT_j가 PT_i로 위장할 수 있다.

이러한 단일 헬퍼 비밀키 문제는 시스템에 등록되는 n명의 사용자마다 서로 다른 헬퍼 비밀키 h_i $(1 \leq i \leq n)$를 발급하여 해결 할 수 있으나, 이 경우 시스템에 등록되는 사용자 수만큼 대응되는 공개키 $P_{HMS_i}=h_iP$들을 모두 HMS의 공개 파라미터에 포함해야 하므로 공개 파라미터의 크기가 증가하는 단점을 가진다.

2) 서비스 제공자에 대한 환자 익명성 저해

Yang 등이 제안한 시스템 모델은 신원기반 암호 기법을 적용하기 위해 사용자의 식별정보가 HMS에게 제공되어야 하며, 헬스케어 서비스를 제공하는 HMS의 신뢰성을 가정하고 있다. 그러나 사용자 관점에서 이는 강한 가정이 될 수 있으며, 비록 서비스 제공자의 신뢰성을 가정하더라도 사용자의 식별정보가 시스템에 부당하게 노출되지 않기를 사용자들은 요구하게 될 것이다.

III. 제안기법

3.1 시스템 모델

Yang 등의 기법에서 드러난 단일 헬퍼 비밀키 문제를 해결하기 위해, 제안기법은 시스템에 등록되는 사용자마다 서로 다른 헬퍼 비밀키를 발급함으로써 어떤 주기의 개인키가 노출되더라도 다음 주기의 개인키를 위조할 수 없도록 한다. 그리고 초기 개인키 생성에 헬퍼 공개키를 바인딩 시킴으로써 사용자를 통해 자신의 헬퍼 공개키를 배포하더라도 임의적으로 헬퍼 공개키를 변조하지 못하도록 하였다. 그리고 각 사용자가 건강기록 전송 프로토콜 수행과정에 자신의 헬퍼 공개키를 포함시킴으로써 HMS가 모든 사용자의 공개키를 시스템의 다른 모든 사용자들에게 배포해야 하는 부담을 줄인다. Fig. 2는 제안 시스템의 구성에 대한 개요를 보여주고 있으며, Table 1은 제안 시스템에서 사용되는 표기에 대해 설명하고 있다.

시스템을 구성하는 각 개체의 역할은 Yang 등의 모델과 유사하며, 본 논문은 사용자의 가명과 보안 파라미터 관리를 위해 신뢰기관인 TA(Trusted Authority)를 추가적으로 가정한다.

Table 1. Notations.

notation	description
G, G_T	bilinear group of a prime order q
$P \in G$	generator of G
$\hat{e}: G \times G \rightarrow G_T$	bilinear pairing
$H_1 : \{0,1\}^* \rightarrow G$	one-way hash function
DT_j	identity of a doctor
PT_i	identity of a patient
pid_i	pseudonym of PT_i
pn_i	registration number of PT_i to HMS
SK_X	id-based private key of X
$s_0 \in Z_q^*$	master secret of TA
$s_1 \in Z_q^*$	master secret of HMS
$h_i \in Z_q^*$	helper secret key for PT_i
$Q_i = h_iP$	helper public key
PHI_i	health information of PT_i
PSK_i^t	private key of PT_i for the t-th period
$IBKIS_{PSK_i^t}()$	id-based key insulated signature under the PSK_i^t
$Enc_K()$	encryption under the key K
$Dec_K()$	decryption under the key K
$MAC_K()$	message authentication code under the key K
ts	time stamp

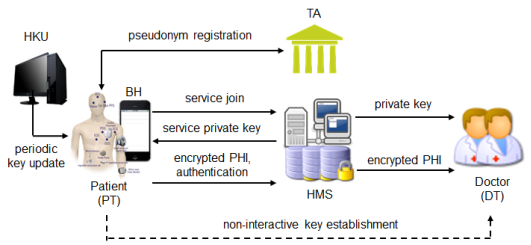

Fig. 2. System model of the proposed scheme.

- TA
  신뢰기관으로서 보안 프로토콜의 수행에 필요한 공개 시스템 파라미터를 생성하여 배포하고, 사용자의 식별정보를 등록하고 서비스 가입에 사용할 가명을 발급한다.

이러한 헬스케어 시스템 모델에 대해 본 논문은 다음과 같은 보안 요구사항들을 고려한다.

- 인증: 시스템에 등록된 정상적인 사용자만이 헬스케어 서비스를 제공받아야 하고, 의사는 수신된 PHI가 등록된 사용자로부터 제공된 정보인지 확신할 수 있어야 한다.
- 익명성: 헬스케어 서비스를 요청하는 사용자의 식별정보가 서비스를 제공받는 동안 부당하게 노출되지 않아야 한다.
- 전송 PHI 보호: 시스템으로 전송되는 사용자의 PHI가 도청으로부터 보호되어야 하고, 환자가 지정한 의사 외에 다른 의사는 해당 PHI에 접근할 수 없어야 한다.

3.2 초기화 (Initialization)

TA는 다음과 같이 마스터 비밀키와 공개 시스템 파라미터를 생성하고 배포한다. 그리고 TA에 등록되는 사용자를 식별하고 사용자의 가명을 발급한다.

1) 시스템의 보안기법에 사용할 겹선형 그룹 파라미터 $(G, G_T, q, P, \hat{e})$를 생성한다.
2) 마스터키로 사용할 $s_0 \in Z_q^*$를 랜덤하게 선택하고, 공개키 $P_{TA} = s_0 P$를 계산한다.
3) 일방향 해시함수 $H_1 : \{0,1\}^* \rightarrow G$를 선택하고, 다음의 공개 시스템 파라미터를 배포한다.
   $params = \langle G, G_T, q, P, \hat{e}, P_{TA}, H_1 \rangle$
4) TA는 등록되는 환자(PT_i)에게 가명 pid_i와 신원기반 개인키 $SK_{PT_i} = s_0 H_1(pid_i)$를 발급하고, $\langle PT_i, pid_i \rangle$를 자신의 데이터베이스에 저장한다.

HMS는 TA의 공개 시스템 파라미터에 따라 다음과 같이 자신의 비밀키를 생성하고, 소속된 의사들에게 개인키를 발급한다.

1) HMS의 마스터키로 사용할 $s_1 \in Z_q^*$을 랜덤하게 선택하고, 공개키 $P_{HMS} = s_1 P$를 계산한다.
2) HMS에 등록된 각 의사 DT_j에게 신원기반 개인키 $SK_{DT_j} = s_1 H_1(DT_j)$를 발급한다.

3.3 등록 (Registration)

헬스케어 서비스를 원하는 환자 PT_i는 다음과 같이 자신의 가명을 HMS에게 등록하고 서비스에 대한 개인키를 발급받는다.

1) 환자는 자신의 pid_i를 사용하여 HMS에게 등록을 요청하고, HMS는 환자가 제시한 pid_i의 유효성을 검사 한다. 이때, 환자의 가명에 대한 유효성 검사는 등록요청 메시지에 환자가 TA로부터 발급받은 SK_{PT_i}를 이용해 신원기반 전자서명을[15-16] 생성하고 HMS는 환자의 pid_i로 서명을 검증함으로써 처리할 수 있다.
2) HMS는 시스템에서 환자 PT_i의 식별에 사용할 등록번호 pn_i을 부여한다. 그리고 헬퍼 개인키 $h_i \in Z_q^*$를 랜덤하게 선택하고 헬퍼 공개키 $Q_i = h_i P$를 계산한 후, PT_i의 초기 개인키 PSK_i^0를 다음과 같이 생성한다.
   $PSK_i^0 = s_1 H_1(pn_i) + h_i H_1(pn_i | Q_i | 0)$
3) HMS는 $\{pn_i, PSK_i^0, h_i, Q_i\}$를 안전한 채널을 통해 환자에게 전송하고, $\langle pid_i, pn_n \rangle$을 자신의 데이터베이스에 저장한다.
4) 환자는 PSK_i^0를 BH로 사용되는 모바일 단말에 저장하고 h_i는 자신의 HKU에 안전하게 보관한다.

3.4 주기별 키 갱신 (Key Evolving)

환자 PT_i는 t번째 주기에 자신의 BH에서 사용할 개인키를 다음과 생성할 수 있다.

1) 자신의 HKU에서 t-주기 임시 헬퍼키 TK_i^t를 다음과 같이 계산하여 BH에게 제공한다.
   $TK_i^t = h_i (H_1(pn_i | Q_i | t) - H_1(pn_i | Q_i | t-1))$
2) BH는 t-주기 개인키 PSK_i^t를 다음과 같이 계산하고, PSK_i^{t-1}와 TK_i^t는 삭제한다.
   $PSK_i^t = PSK_i^{t-1} + TK_i^t$

3.5 건강기록 전송 (PHI transmission)

환자 PT_i는 자신의 건강정보 PHI_i를 진단하기를 원하는 의사 DT_j를 선택하고, 다음과 같이 자신의 건강정보에 대한 보안처리를 수행하여 HMS를 통해 의사에게 제공한다.

1) 환자 PT_i는 HMS에 등록된 의사 DT_j를 선택하고, HKU에서 $DP_i^j = h_i H_1(DT_j)$를 계산하여 BH에 저장한다. 이 과정은 의사를 선택하는 초기 단계에서 한 번만 수행하면 된다.
2) 현재 대응되는 시스템의 주기가 t라 할 때, 환자는 의사와 비대화식으로 공유하게 될 비밀키 k_{PD}를 다음과 같이 계산한다. 이때 KDF는 키 유도함수(Key Derivation Function)를 의미한다.
$K = \hat{e}(PSK_i^t, H_1(DT_j))$
$k_{PD,0} = KDF(K|0)$, $k_{PD,1} = KDF(K|1)$
3) 환자는 자신의 건강기록 전송을 위한 메시지 $msg = \{pn_i, Q_i, DP_i^j, ts, DT_j, C_1, C_2\}$ 를 구성하고 $msg|\sigma$를 HMS로 전달한다. 이때 C_1, C_2, σ는 각각 다음과 같이 생성된다.
- $C_1 = Enc_{k_{PD,0}}(PHI_i, ts)$
- $C_2 = MAC_{k_{PD,1}}(pn_i, Q_i, DP_i^j, ts, DT_j, C_1)$
- $\sigma = IBKIS_{PSK_i^t}(msg)$

환자로부터 $msg|\sigma$를 수신한 HMS는 먼저 pn_i로 등록된 환자의 전자서명 σ를 검증하고[13], 서명이 올바른 경우 msg를 지정된 의사 DT_j에게 전달한다. 그러면 HMS를 통해 전달된 msg를 수신한 의사 DT_j는 다음과 같이 환자의 PHI_i를 추출한다.

1) 의사는 pn_i 환자와 t주기에 공유하게 되는 비밀키를 다음과 같이 계산한다.
$K' = \hat{e}(H_1(pn_i), SK_{DT_j})\,\hat{e}(H_1(pn_i|Q_i|t), DP_i^j)$
$k'_{PD,0} = KDF(K|0)$, $k'_{PD,1} = KDF(K|1)$
2) 의사는 $C_2 = MAC_{k'_{PD,1}}(pn_i, Q_i, DP_i^j, ts, DT_j, C_1)$ 여부를 검증하고, $Dec_{k'_{PD,0}}(C_1)$ 복호화를 통해 환자의 건강정보 PHI_i를 획득한다.

다음 계산식을 통해서 환자와 의사가 각각 계산한 키 K와 K'가 일치함을 보일 수 있다.

$$\begin{aligned}
K &= \hat{e}(PSK_i^t, H_1(DT_j)) \\
&= \hat{e}(s_1 H_1(pn_i) + h_i H_2(pn_i|Q_i|t), H_1(DT_j)) \\
&= \hat{e}(s_1 H_1(pn_i), H_1(DT_j))\,\hat{e}(h_i H_1(pn_i|Q_i|t), H_1(DT_j)) \\
&= \hat{e}(H_1(pn_i), s_1 H_1(DT_j))\,\hat{e}(H_1(pn_i|Q_i|t), h_i H_1(DT_j)) \\
&= \hat{e}(H_1(pn_i), SK_{DT_j})\,\hat{e}(H_1(pn_i|Q_i|t), DP_i^j) \\
&= K'
\end{aligned}$$

IV. 분 석

4.1 안전성

본 절에서는 제안된 기법이 보안 요구사항들을 어떻게 만족하는지 논의한다. Table 2는 [5]와 [8]에서 각각 제시된 Lin 등과 Yang 등의 기법과 본 논문의 제안기법이 제공하는 보안기능들을 간략하게 비교하여 나타내고 있다. Table 2에 제시된 각 보안기능 평가항목은 다음과 같다.

Ⅰ: 인증 (Authentication)
Ⅱ: 키 격리 (Key-insulation)
Ⅲ-1: HMS에 대한 환자 익명성 (Patient's anonymity to HMS)
Ⅲ-2: 의사에 대한 환자 익명성 (Patient's anonymity to doctor)

Lin 등은 스마트폰을 활용한 안전한 건강기록 전송을 위해 가명과 신원기반 암호기법을 이용한 익명인증과 건강기록 전송보안 기법을 제안하였다. 그러나 Lin 등은 스마트폰에서 사용할 개인키의 주기적 갱신에 대해서는 고려하지 않았으며, 이에 대해 Yang 등은 스마트폰과 같은 휴대용 단말의 분실로 인한 개인키 노출문제가 발생할 수 있음을 언급하고 개인키 노출로 인한 이 후의 위장이나 위조 등의 피해를 줄이기 위해 주기적으로 스마트폰에서 사용할 개인키를 갱신할 수 있는 키 격리 기법을 적용한 방안을 제안하였다. 그러나 앞서 Ⅱ장에서 논의한바와

Table 2. Security comparisons.

	Lin et al.	Yang et al.	Proposed
Ⅰ	√	√	√
Ⅱ			√
Ⅲ-1	√		√
Ⅲ-2	√	√	√

같이, 저자들의 주장과 달리 Yang 등의 기법은 잘 못 구성된 보안 파라미터와 프로토콜 설계로 인해 안전한 키 격리 방법을 제공하지 못한다. 그리고 프로토콜 수행단계에서 환자의 식별정보가 그대로 HMS에게 제공되므로 환자의 익명성도 보장하지 못한다.

• 인증

제안기법은 키 격리 전자서명 기법[13]과 메시지 인증코드를 통해 헬스케어 시스템에 등록된 사용자만이 정상적인 서비스를 제공받을 수 있도록 보장할 수 있다. 사용자의 PHI를 전송하는 단계에서, 사용자는 건강정보를 포함하는 메시지 msg를 HMS로 전송하기 위해 전자서명 $IBKIS_{PSK_i^t}(msg)$을 첨부해야 한다. 이때 전자서명을 위한 t주기 개인키 PSK_i^t는 등록단계에서 HMS를 통해 등록번호 pn_i에 대해 HMS의 마스터 비밀키를 이용하여 생성된 초기 개인키 PSK_i^0를 획득한 사용자만이 계산할 수 있다. 따라서 키 격리 전자서명 기법의 안전성을 가정할 때 정상적인 등록과정을 거치지 않은 사용자는 헬스케어 서비스를 제공받을 수 없다.

또한 사용자 마다 서로 다른 헬퍼 비밀키 h_i가 발급되고, 개인키 $PSK_i^0 = s_1 H_1(pn_i) + h_i H_1(pn_i|Q_i|0)$에 헬퍼 공개키 $Q_i = h_i P$가 결합되므로 t-주기에 PT_i의 개인키 PSK_i^t가 노출될지라도 PT_i이외의 다른 사용자가 헬퍼 비밀키 h_i를 위변조하거나 t-주기 이후의 개인키를 조작할 수 없다. 따라서 Yang 등의 기법에서 발생할 수 있는 문제를 해결할 수 있다.

그리고 의사에게 전달되는 사용자의 건강정보 PHI_i는 비대화식 키 설정기법에 따라 사용자와 의사 사이에 공유되는 비밀키를 이용하여 암호화되고 메시지 인증코드를 포함한다. 따라서 의사는 메시지 인증코드를 검증함으로써 메시지에 명시된 사용자 등록번호 pn_i에 대응되는 개인키 PSK_i^t를 가진 정상적인 사용자가 전송한 건강정보임을 인증할 수 있다.

• 익명성

제안 시스템에서 환자의 익명성은 환자의 식별정보 PT_i에 대해 TA가 발급한 가명 pid_i와 HMS가 발급한 등록번호 pn_i를 통해 보장 받을 수 있다. TA와 HMS로부터 pid_i와 pn_i가 각각 안전한 채널을 통해 발급되었다고 가정할 때, HMS는 등록과정에서 환자가 제시하는 가명 pid_i에 대응되는 식별정보 PT_i는 직접적으로 확인할 수 없으며 TA가 발급한 pid_i의 유효성만 검사할 수 있다. 그리고 TA는 HMS의 헬스케어 서비스에 사용되는 pn_i가 누구인지를 직접적으로 식별할 수 없다.

그러나 정상적인 서비스 환경에서는 환자의 프라이버시 보호를 위해 익명성이 보장되어야 하지만, 건강정보의 진단을 통해 심각한 문제가 발견되거나 역학조사가 필요한 경우에는 해당 환자의 추적이 필요할 수도 있다. 즉, 문제의 소지가 있는 상황에 대비한 조건부 프라이버시 보호가 필요하다. 이러한 경우에 한해서 HMS는 TA와 협력을 통해 자신들이 보관하고 있는 $\langle pn_i, pid_i \rangle$와 $\langle PT_i, pid_i \rangle$를 연관시킴으로써 문제의 소지가 있는 환자의 식별정보를 추적할 수 있다.

• 전송 PHI 보호

HMS를 통해 의사 DT_j에게 전달되는 사용자 PT_i의 건강정보는 PT_i와 DT_j 사이에 공유되는 비밀키를 이용하여 암호화되어 전송된다. 따라서 신원기반 비대화식 공유 비밀키 설정기법의 안전성을 가정할 때, 네트워크 도청으로부터 전송되는 건강정보 메시지의 기밀성을 보장할 수 있다.

또한 공유 비밀키는 $K = \hat{e}(PSK_i^t, H_1(DT_j)) = \hat{e}(H_1(pn_i, SK_{DT_j}))\hat{e}(H_1(pn_i|Q_i|t), DP_i^j)$와 같이 계산되므로, 환자가 자신의 건강정보 진단을 위해 지정한 의사 식별정보 DT_j에 대한 신원기반 개인키 $SK_{DT_j} = s_1 H_1(DT_j)$를 소유한 해당 의사만 환자의 건강정보에 접근할 수 있고 제 삼자는 건강정보에 접근할 수 없다.

4.2 성능

Table 3은 안전한 개인 건강기록 전송 프로토콜에 대한 제안기법의 효율성을 Yang 등의 기법과 비교하여 나타내고 있다. 보안처리를 위한 주요 연산으로 비대화식 키 설정과 인증을 위한 신원기반 암호기법의 겹선형 페어링(T_p)과 스칼라 곱셈(T_m), 비밀키 암호화(T_e)와 복호화(T_d) 연산 그리고 프로토콜 수행에 따른 통신횟수(communication rounds)로 평가하였다. 통신횟수와 관련하여, Yang 등의 기법은 환자가 의사에게 건강기록을 전송단계에서 먼

저 HMS를 통해 환자의 가명과 개인키를 발급받은 이 후에 환자와 의사 사이의 건강기록 전송보안 프로토콜이 수행되므로 총 3 라운드의 통신이 필요하다. 반면 본 논문에서 제안된 기법은 사전에 미리 환자의 가명 개인키가 발급되므로 환자와 의사 사이의 건강기록 전송보안은 1 라운드의 통신으로 처리 될 수 있다.

Yang 등의 기법은 3 라운드 과정에서 BH와 HMS, HMS와 DT, BH와 DT 사이의 각각 비대화식 공유 비밀키 설정을 위한 연산이 소요된 결과이다. 제안기법의 BH와 HMS의 연산량은 키 격리 서명생성과 검증[13]을 포함한 결과이다. 그리고 겹선형 페어링 기반의 암호연산의 성능평가를 위해 공개암호 라이브러리 jPBC에서 제공하는 512비트 소수 p의 F_p에서 160비트 소수 q를 위수(subgroup order)로 하는 타원곡선상에서 정의된 겹선형 페어링 연산을 이용하였다[17]. 또한 BH의 성능분석은 사용자 스마트폰 단말 환경을 고려하여 갤럭시 S4 기기에서 측정된 성능지표를 고려하였고, 이에 반해 HMS와 DT의 성능은 쿼드코어2 CPU 2.4GHz PC에서 측정된 지표를 고려하였다.

Table 3의 결과에서 보여주듯이, 건강기록 전송을 위한 사용자의 BH 역할을 스마트폰과 같은 모바일 단말이 수행한다고 가정할 때, 제안기법이 Yang 등의 기법보다 효율적으로 프로토콜을 수행할 수 있음을 알 수 있다. 그리고 HMS의 성능과 관련하여, 암호연산 수행 소요시간만으로는 Yang 등의 기법이 조금 더 효율적이나, Yang 등의 기법은 환자의 건강기록 전송과정이 3라운드로 이루어지므로 통신지연을 포함하여 전체적인 성능을 고려한다면 제안기법이 보다 효율적으로 인증과 건강기록 전송보안을 처리할 수 있다.

Table 3. Efficiency of the proposed scheme for secure PHI transmission (time: ms).

Yang et al.		
BH	$2T_p+2T_e+1T_d$	≈418.4
HMS	$3T_p+2T_e+1T_d$	≈21.7
DT	$2T_p+2T_d$	≈14.6
comm.	3 round	
Proposed		
BH	$1T_p+2T_m+1T_e$	≈276.4
HMS	$4T_p$	≈28.9
DT	$2T_p+1T_d$	≈14.5
comm.	1 round	

V. 결 론

스마트 헬스케어 기술에 대한 관심의 증가와 웨어러블 디바이스의 발전으로 인해 최근 WBN을 활용한 원격지 건강정보 모니터링 서비스가 주목받고 있다. 그러나 네트워크를 통해 전송되는 사용자의 개인건강기록에 대한 보호가 필요하며, 환자의 개인 식별정보나 건강기록이 부당하게 노출되지 않도록 환자의 프라이버시도 반드시 보호되어야 한다. 이에 본 논문에서는 원격 건강정보 모니터링 시스템을 위해 Yang 등이 제시한 익명 인증기법의 잘못 설계된 키 격리 기법의 보안문제와 환자의 익명성 저해문제에 대해 고찰하였다. 그리고 이러한 보안 문제를 해결하기 위해 본 논문은 사용자마다 주기적인 개인키 갱신을 위한 서로 다른 헬퍼 비밀키를 관리하고 신뢰기관을 통해 발급된 가명을 통해 익명성을 보장할 수 있는 원격 건강정보 시스템의 익명인증 기법을 제안하였다. 본 논문에서 제안된 익명인증 기법을 적용함으로써 모바일 단말을 통해 건강관리 모니터링 시스템으로 전송되는 개인 건강정보에 대한 보안성을 향상시킬 수 있을 뿐만 아니라, 개인 민감정보의 전송이 요구되는 유사한 모바일 응용서비스 환경에도 본 논문에서 논의한 익명인증 기법의 원리를 적용할 수 있을 것으로 기대한다. 아울러 본 논문에서는 환자에 의해 지정된 한 명의 의사에게만 건강정보를 전송하는 환경을 가정하였으나, 향후 협업 의료서비스 환경도 고려하여 환자의 건강진단에 관련된 여러 의료진들에게 건강정보를 안전하게 전송하기 위한 효율적인 보안기법의 연구가 필요할 것으로 사료된다.

References

[1] C.-T. Li, C.-Y. Weng, C.-C. Lee, and C-C Wang, "Secure user authentication and user anonymity scheme based on quadratic residues for the integrated EPRIS," Procedia Computer Science, vol. 52, pp. 21-28, Jun. 2015.

[2] F. Wen, "A more secure anonymous user authentication scheme for the integrated EPR information system", Journal of Medical Systems, vol. 38, no. 5, pp. 1-7, May. 2014.

[3] Q. Jiang, J. Ma, Z. Ma, and G. Li, "A pri-

vacy enhanced authentication scheme for telecare medical information systems," Journal of Medical Systems, vol. 37, no. 1, pp. 1-8, Feb. 2013.

[4] H. M. Chen, J. W. Lo, and C. K. Yeh, "An efficient and secure dynamic id-based authentication scheme for telecare medical information systems", Journal of Medical Systems, vol. 36, no. 6, pp. 3907-3915, Dec. 2012.

[5] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for eHealth systems," IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 365-378, May. 2009.

[6] X. Liang, M. Barua, R. Lu, and X. S. "Privacy-preserving wireless data transmission for e-healthcare applications," IEEE COMSOC MMTC E-Letter, vol. 6, no. 11, pp. 39-41, Nov. 2011.

[7] L. Guo, C. Zhang, J. Sun, and Y. Fang, "PAAS: A Privacy-preserving attribute-based authentication System for eHealth Networks," IEEE International Conference on Distributed Computing Systems, pp. 224-233, Jun. 2012.

[8] H. Yang, H. Kim, and K Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system," Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1059-1069, Nov. 2014.

[9] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Annual International Cryptology Conference – CRYPTO 2001, pp. 213-229, Aug. 2001.

[10] N. P. Smart, "An identity-based key agreement protocol based on Weil pairing," Electronic Letters, vol. 38, no. 13, pp. 630-632, Jun. 2002.

[11] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Strong key-insulated signature schemes," International Conference on Theory and Practice in Public Key Cryptography - PKC 2003, pp. 130-144, Jan. 2003.

[12] J. Weng, S. Liu, K. Chen, and X. Li, "Identity-based key-insulated signature with secure key-updates," International Conference on Information Security and Cryptology - Inscrypt 2006, pp.13-26, Nov. 2006.

[13] P. V. S. S. N. Gopal and P. Vasudeva Reddy, "Efficient id-based key-insulated signature scheme with batch verifications using bilinear pairings over elliptic curve," Journal of Discrete Mathematical Sciences and Cryptography, vol. 18, no. 4, pp. 385-402, Jul. 2015.

[14] R. Dupont and A. Enge, "Provably secure non-interactive key distribution based on pairings," Discrete Applied Mathematics, vol. 154, no. 2, pp. 270-276, Feb. 2006.

[15] J. Cha, J and Cheon "An identity-based signature from gap Diffie-Hellman groups," International Conference on Theory and Practice in Public Key Cryptography - PKC 2003, pp. 18-30, Jan. 2003.

[16] C. Gentry, A. Silverberg, "Hierarchical id-based cryptography," International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT 2002, pp. 548-566, Dec. 2002.

[17] A. De Caro and V. Iovino, "jPBC: Java pairing based cryptography," Proceedings of the 16th IEEE Symposium on Computers and Communications, pp. 850-855, Jun. 2011.

〈저 자 소 개〉

박 영 호 (Youngho Park) 정회원
2000년 2월: 부경대학교 전자계산학과 졸업
2002년 2월: 부경대학교 대학원 전자계산학과 석사
2006년 8월: 부경대학교 대학원 정보보호학(협) 박사
2014년 7월~현재: 부경대학교 전자정보통신연구소 전임연구원
〈관심분야〉 정보보호, 암호기술 응용, 통신보안, 인증, 키 관리

노 시 완 (Si-Wan Noh) 학생회원
2016년 2월: 부경대학교 IT융합응용공학과 졸업
2016년 3월~현재: 부경대학교 대학원 정보보호학(협) 석사과정
〈관심분야〉 정보보호, 차량통신보안, 헬스케어 보안

이 경 현 (Kyung-Hyune Rhee) 종신회원
1982년 2월: 경북대학교 수학교육과 졸업
1985년 2월: 한국과학기술원 응용수학과 석사
1992년 8월: 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재: 부경대학 IT융합응용공학과 교수
〈관심분야〉 정보보호, 암호이론, 암호 프로토콜, 통신보안