홈 네트워크 환경의 안전한 모바일 헬스케어 서비스 방식 제안

서대희*, 이임영*
*순천향대학교 정보기술공학부
e-mail:1636711@hitel.net

A Study on secure mobile hearth care service for homenetwork

Dae-Hee Seo*, Im-Yeong Lee*
*Division of Information Technology Engineering
SoonChunHyang University

요약

최근 인터넷의 급성장에 따라 유·무선 네트워크 기반의 다양한 서비스들이 소개되고 서비스 되고 있다. 그 중에서도 사용자의 건강과 관련된 서비스가 헬스케어 서비스이다. 특히, 모바일 단말기 보급과 더불어 건강에 대한 관심은 모바일 헬스케어 서비스에 대한 연구를 촉진시키고 있는 실정이다. 따라서 본 연구에서는 기존의 모바일 헬스케어 서비스에서 보안적 취약점을 분석하고 홈 네트워크 환경에서 모바일 헬스케어 서비스를 제공할 경우 요구되는 보안적인 요구사항을 제시하여 홈 네트워크 기반의 안전한 모바일 헬스케어 서비스를 제안하고자 한다.

1. 서 론

인터넷의 급속한 확산은 기존 오프라인 서비스의 온라인화를 가속시켰으며, 모바일 단말기의 대중화는 유선에서 무선으로 변화하는 사용자 서비스 욕구를 대변하고 있다.

특히, 최근 들어 관심의 초점은 삶의 질과 관련되어 건강과 가장 밀접한 관계가 있으며, 이와 연관된 어플리케이션 서비스가 헬스케어 서비스이다.

기존의 단순한 모니터링 기능에 한정된 헬스케어 서비스가 모바일 단말기의 보급과 관련되어 이동성을 통한 높은 질의 어플리케이션 서비스로 변화하는 연구가 많이 진행중에 있다.

본 논문에서는 홈 네트워크 상태에서 사용자의 모바일 단말기를 통한 안전한 모바일 헬스케어 서비스를 제안하고자 한다. 본 논문의 2장에서는 모바일 헬스케어 서비스의 개요와 보안의 필요성을 기술하고 이를 만족할 수 있는 보안 요구사항 제시하고자 한다. 3장에서는 기존의 모바일 헬스케어 서비스에 대한 보안 분석을 수행한 뒤 4장에서는 2장에서의 보안 요구사항을 만족할 수 있는 안전한 모바일 헬스케어 서비스를 제안한다. 5장에서는 제안된 방식을 기존 방식과 비교 분석한 뒤 6장에서 결론을 맺고자 한다.

2. 모바일 헬스케어 서비스와 보안 요구사항

2.1 모바일 헬스케어 서비스

헬스케어 서비스는 사용자의 건강과 관련되어 예방, 치료, 질병관리, 정신적 육체적인 안정유지등의 서비스를 제공하는 인터넷 어플리케이션 서비스를 의미한다. 초기의 헬스케어 서비스는 독립적인 헬스케어 서비스로써 사용자가 오프라인으로 병원에서 진단과 치료를 수행하는 서비스였다. 그러나 모바일 단말기의 급속한 확산과 더불어 초고속 인터넷의 보급은 기존의 서비스와는 차별화 되면서 전자적인 데이터 교환을 통한 분산된 환경에서의 모바일 헬스케어 서비스를 가능하게 하였다. 모바일 헬스케어의 경우 자동화된 디바이스를 통해 사용자의 상태를 지속적으로 모니터링할 뿐만 아니라 이상 징후 발생시 이를 곧바로 해당 의료기관에 통보함으로써 위급한 상황에 신속히 대처할 수 있도록 하는 유용한 어플리케이션 서비스이다.

2.2 모바일 헬스케어 서비스의 보안 요구사항

모바일 헬스케어 서비스의 경우 정당한 서비스 요구자에게 환자의 건강 정보를 전송하여 지속적인 모니터링이나 응급사항이 발생되었을 시 신속한 대처나

빠른 조치를 취하기 위한 부가가치 서비스이다.
그러나 이는 사용자의 개인정보와 매우 밀접한 관계가 있으며, 이에 대한 보안 서비스가 제공되지 않을 경우 악의적인 사용자에 의해 정당한 사용자의 프라이버시 정보가 악용될 수 있다. 따라서 모바일 헬스케어 서비스를 제공하기 위해서는 다음과 같은 보안 사항이 요구되며, 이는 다음과 같다.
- 인증 : 모바엘 헬스케어 사용자에 대한 정당한 인증은 개인의 프라이버시 정보를 보호하기 위해 반드시 필요한 요구조건이며, 프로토콜의 참여자와의 상호 인증은 악의적인 제 3자의 인증 공격에 보안할 수 있다.
- 기밀성과 무결성 : 모바일 헬스케어 서비스에서 전송되는 정보중 개인의 프라이버시 정보와 그에 대한 응답 메시지는 불법 사용자에 의해 도청이나 위조 변조 되서는 안되며, 이를 위해 전송 데이터의 기밀성과 무결성이 제공되어야 한다.
- 접근 제어 : 사용자의 모바일 헬스케어 정보가 저장된 저장소에 대한 보안적인 접근 제어 서비스는 향후 발생할 수 있는 시스템의 안전성을 위해 반드시 요구되는 보안 요구사항이다.
- 독립성 : 사용자의 모바일 디바이스에 저장된 정보는 모바일 헬스케어 서비스의 저장소와는 독립성을 유지하여 기밀된 정보를 유지할 수 있어야 한다. 이는 모바일 헬스케어 서비스의 저장소에 저장된 정보를 이용하여 사용자의 프라이버시 정보를 할 수 있는 보안적 취약점을 보완하기 위한 요구사항이다.

3. 기존 모바일 헬스케어 서비스 방식 분석

본 장에서는 모바일 헬스케어 서비스와 관계된 기존 방식들을 살펴본 뒤 이에 대한 보안 취약점을 분석하고자 한다.

① Security in a Wireless Mobile Health Care System

본 방식의 경우 모바일 헬스케어 서비스의 보안 서비스를 위한 방식을 제안하였다. 그러나 다음과 같은 보안적 취약점을 내포하고 있다.

- 인증 : 사용자의 인증은 수행하지 않으며, 모바일 기기에 대한 통신 인증만을 수행함으로써 불법 사용자에 의한 인증 공격에 취약점을 나타내고 있다.

- 기밀성과 무결성 : 논문에서 제기된 방식은 SSL 혹은 HTTPS 프로토콜을 이용하여 인증을 수행함으로써 기존 SSL이나 HTTPS의 기밀성과 무결성과 관련된 취약성을 그대로 내포하고 있다.

② MobiHealth-innovative 2.5/3G mobile service and application for healthcare

본 방식은 근거리 무선 통신 기술을 이용하여 모바일 헬스케어 서비스를 제공하는 방식을 제안하였으나 다음과 같은 보안적 취약점이 문제시 되고 있다.

- 인증 : 사용자의 인증을 수행하지 않고 모바일 디바이스에 대한 개체 인증만을 수행하여 불법 사용자에 대한 보안 대책이 없다.

- 기밀성과 무결성 : 근거리 무선 통신 방식을 그대로 적용하여 기존 시스템의 보안 취약점을 그대로 내포하고 있다.

③ Ubiquitous Healthcare : The Onkonet Mobile Agents Architecture

본 방식의 경우 에이전트 기반의 모바일 헬스케어 서비스를 제안하였다. 그러나 다음과 같은 보안적 취약점을 제시할 수 있다.(본 논문에서는 에이전트의 보안 취약점에 대해서는 기술하지 않는다.)

- 접근제어 : 본 방식에서는 멀티 에이전트를 이용해 사용자의 접근 제어를 제공하였으나 이는 저장소에 대한 기밀 저장 서비스를 제공하지 않아 보안적 취약점이 발생하고 있다.

- 독립성 : 본 방식은 멀티 에이전트 시스템과 모바일 헬스케어 서비스 저장소와 공통된 저장소를 사용함으로써 사용자의 프라이버시 정보를 보호할 수 없다.

4. 홈 네트워크 환경에서의 안전한 모바일 헬스케어 서비스 방식 제안

본 제안방식은 홈 네트워크 구조하에서 개인의 헬스케어 정보를 모바일 디바이스를 통해 모바일 헬스케어 서비스 서버로부터의 주기적인 모니터링을 통해 사용자의 헬스케어 정보를 안전하고 효율적으로 관리하는 방식을 제안하였으며, 다음과 같은 3개의 개체로 구성된다.
- 모바일 디바이스 : 모바일 디바이스는 홈 네트워크 내부에서 모바일성을 지닌 디바이스로써 사용자의 헬스케어 정보를 홈 게이트웨이에 전송하는 개체이다.
- 홈게이트 웨이 : 모바일 디바이스와 모바일 헬스케어 서버와의 상호 인증을 통해 각각의 개체를 인증하고 모바일 헬스케어 서버와 모바일 디바이스의 통신을 중계하는 개체이다.
- 모바일 헬스케어 서버 : 사용자의 모바일 디바이스에서 전송되어온 헬스케어 정보를 이용해 해당 의사나 병원에 이를 전송하고 그에 대한 응답 메시지를 해당 홈 게이트웨이에 전송하는 개체이다.

4.1 시스템 계수

(* : u - 사용자, w - 홈 게이트웨이, d - 모바일 디바이스, s - 모바일 헬스케어 서버

p, q : p는 소수, $q = q|p-1$

PI_* : 사용자의 프라이버시 정보

$E()$: 공개키 암호 알고리즘

$H()$: 안전한 해쉬 함수

T_* : 타임 스탬프

4.2 사전 전제사항

모바일 헬스케어를 제공받고자 하는 사용자는 사전에 사용자의 개인 정보와 모바일 디바이스 고유의 PIN번호를 이용해 안전한 해쉬 값을 다음과 같이 생성한 뒤 이를 홈 네트워크(PI_1)와 모바일 헬스케어 서버(PI_2)에 각각 안전하게 등록하고 v는 사용자만이 관리한다.

$$PI_1 = H(Privacyinformation||T_u)$$

$$PI_2 = H(MobilePIN||T_u)$$

$$v = g^{PI_1} * g^{PI_2}$$

4.3 프로토콜

제안방식은 사용자의 헬스케어 정보를 병원이나 의사가 주기적인 모니터링을 수행하는 프로토콜을 제안하도록 한다.

① 사용자는 자신의 주변 혹은 신체에 부착된 모바일 기기의 ID와 헬스케어 요청 메시지 M, 그리고 다음과 같이 K_1을 계산하여 이를 홈 네트워크 게이트웨이에 전송한다.

$$K_1 = g_1^{PI_1} \ mod \ p$$

② 홈네트워크 게이트웨이는 전송 받은 K_1을 이용하여 K를 생성하고 모바일 디바이스에서 전송된 사용자의 헬스케어 요청 메시지 M과 타임 스탬프 T_w, 암호화된 V를 모바일 헬스케어 서버에 전송한다.

$$K = K_1 * g^{r_w} \ mod \ p$$

$$V = E_{s_p}(r_w||T_w)$$

③ 모바일 헬스케어 서버는 홈 네트워크 게이트웨이로부터 전송되어온 V, K, M, T_w를 다음과 같은 검증과정을 거쳐 그 정당성을 확인한 뒤 V_1, y_2, x_2를 계산하여 사용자의 모바일 헬스케어 서비스 요청 메시지에 해당되는 응답 메시지를 M_{res}를 생성하여 타임 스탬프 T_s와 함께 홈네트워크 게이트웨이에 전송한다.

- 검증과정

V를 자신의 개인키로 복호화 하여 r_w을 추출한 사전에 사용자가 등록한 사용자 정보 PI_2를 이용해 K'를 생성하여 전송되어온 K와 비교하여 정당성을 확인한다.

$$K' = g^{PI_2} * g^{r_w} \ mod \ p$$

- 홈네트워크 게이트웨이 전송을 위한 V_1, x_1, y_2의 연산 과정을 수행하여 전송한다.

$$V_1 = E_{w_p}(e||M_{res})$$

$$x_1 = g^{r_2} \ mod \ p$$

$$y_2 = (r_2 + ePI_2) \ mod \ q$$

④ 홈네트워크 게이트웨이는 모바일 헬스케어 서버로부터 전송되어온 정보에서 V_1을 자신의 개인키로 복호화하여 e를 추출한 뒤 y_1을 계산하여 $(y_1||y_2)$, V_2, x와 함께 사용자의 주변 혹은 신체에 부착된 모바일기기에 이를 전송한다.

$$V_2 = E_{d_p}(e||M_{res}||T_H)$$

$$x = x_1 * g^{r_1} mod \ p$$

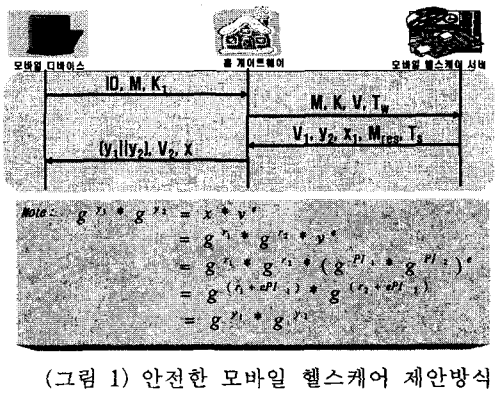
$$y_1 = (r_1 + ePI_1) \ mod \ q$$

⑤ V_2와 y_1, x를 전송 받은 사용자는의 모바일 기기 자신의 개인키로 V_2를 복호화하여 e를 추출한 뒤 사용자만이 관리하는 v를 이용해 검증과정을 수행한다. 사용자는 검증 과정이 올바른 경우 M_{res}를 추출함으로써 모바일 헬스케어 서비스를 제공 받는다.

<검증 과정>

$$\begin{aligned} g^{y_1} * g^{y_2} = x^* v^e \\ &= g^{r_1} * g^{r_2} * v^e \\ &= g^{r_1} * g^{r_2} * (g^{PI_1} * g^{PI_2})^e \\ &= g^{(r_1 + ePI_1)} * g^{(r_2 + ePI_2)} \\ &= g^{y_1} * g^{y_2} \end{aligned}$$

이상의 과정을 다음과 같이 그림 1로 도해시 할 수 있다.



(그림 1) 안전한 모바일 헬스케어 제안방식

5. 제안방식 비교 분석

본 제안 방식은 2장에서 제시한 보안 요구사항을 다음과 같이 만족한다.

- 인증 : 사용자의 프라이버시 정보가 안전하게 등록되는 가정을 기반으로 하여 프라이버시 정보를 이용한 검증 과정을 통해 사용자의 안전한 인증 과정을 수행한다.
- 기밀성과 무결성 : 제안된 방식은 이산대수의 어려움에 근거한 연산을 통해 사용자의 기밀성을 유지할 수 있도록 하였으며, 초기 사용자의 프라이버시 등록시 생성되는 *PI*정보를 안전한 해쉬 값으로 생성함으로써 무결성을 유지하도록 하였다.
- 접근 제어 : 본 논문에서 사용자의 모바일 헬스케어 정보가 저장된 저장소에 대한 보안적인 접근 제어 서비스는 사용자의 모바일 디바이스의 *PIN*정보에 대한 해쉬 값을 기반으로 하여 불법 사용자에 대한 사용자 정보의 불법적 접근을 제어함으로써 보안적 안전성을 유지하였다.
- 독립성 : 사용자의 모바일 디바이스에 저장된 정보는 모바일 헬스케어 서비스의 저장소와는 독립성을 유지하여 기밀된 정보를 유지할 수 있어야 한다. 이는 모바일 헬스케어 서비스의 저장소에 저장된 정보를 이용하여 사용자의 프라이버시 정보를 할 수 있는 보안적 취약점을 보완하기 위한 요구사항이다. 사용자의 모바일 디바이스와 모바일 헬스케어 서비스 저장소에 저장되는 정보가 각각 구분되어 등록되어 헬스케어 서비스의 요청시 연산에 활용되어 검증 과정을 제시함으로써 각 개체간의 독립성을 제공하였다.

6. 결론

최근 정보통신의 급속한 발전은 다양한 어플리케이션의 연구를 촉진시키는 계기가 되었으며, 사용자의 욕구 또한 단순한 정보 전송의 서비스가 아닌 다양한 서비스 형태를 요구하고 있다.

본 논문에서는 사용자의 건강에 대한 인식의 전환에 따른 어플리케이션 서비스 중의 하나인 헬스케어 서비스를 홈 네트워크 환경에 적용하였다.

제안된 방식의 경우 사용자의 프라이버시 정보를 안전하게 저장 후 사용함으로써 기존의 헬스케어 서비스에서 문제시 되고 있는 보안적 취약점을 보완하였다. 그러나 모바일 환경의 적용에 따른 연산량은 미흡한 부분이라 할 수 있겠다.

향후 연구 방향으로써는 유비쿼터스 컴퓨팅 환경에 적합한 헬스케어 서비스와 연산량의 경량화 및 자동화 서비스를 위한 연구가 추가적으로 수행될 예정이다.

6. 참고문헌

[1]. ANSI X9.42, "Agreement of sysmmetric Key on Using Diffie-Hellman Cryptography", 2001

[2]. ANSI X9.63, "Public Key Cryptography for the finanacial service industry : key agreement and key transport using elliptic curve cryptography", 2001

[3]. C.J. Mitchell, M.Ward, P. Wilson, "Key control in key agreement protocols", Electronics Letters 14th, Vol.34, No.10, May, 1998

[4]. Y. Dodis, S.Micali, "Parallel Reducibility for Information Theoretically Secure Computation", CRYPTO '00, 2000

[5]. S.J. Kim, M. Mambo et al, "On the security of the Okamoto-Tanaka ID-Based Key Exchange scheme against Active attacks", IEICE Trans, pp231-238, Jan. 2001

[6]. Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY", CRC, 1996

[7]. 이임영 "전자상거래 보안입문", 생능출판사, 2001