The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 6, pp.163-171, Dec. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.6.163
JIIBC 2015-6-23

개인건강기록 서비스에서 보안취약성 및 위협요소에 관한 연구

A Study on Security Weakness and Threats in Personal Health Record Services

이명규*, 황희정**

Myung-Kyu Yi*, Hee-Joung Hwang**

요 약 개인건강기록 서비스는 환자에게 건강기록 관리와 중요한 의료파일 관리 그리고 응급상황 연락과 같이 편리하고 사용하기 쉬운 해결책을 제시해준다. 이러한 중요한 장점에도 불구하고 개인건강기록 서비스는 데이터의 보안에 관련된 소비자 입장에서는 피할 수 없는 중요한 도전을 제기하고 있다. 개인건강기록 기술이 헬스케어와 융합되면서 사용자 개인정보 침해가 발생하고 사용자의 민감한 의료정보가 유출되는 문제가 증가되고 있다. 본 논문에서는 개인건강기록 서비스의 취약점과 반드시 해결해야할 다양한 보안 측면을 분석한다. 또한, 개인건강기록 사용자와 애플리케이션 서비스 제공자 관점에서 보안 요구사항을 기술하였으며, 개인건강기록 보안 요구사항을 만족하고 보안위협을 대응할 수 있는 보안 메커니즘에 대해 연구하였다

Abstract Personal Health Records(PHR) service offers patients a convenient and easy-to-use solution for managing their personal health records, crucial medical files, and emergency contacts. In spite of the indispensable advantages, PHR service brings critical challenges that cannot be avoided from consumer side if the security of the data is concerned. The problem of user's privacy infringement and leaking user's sensitive medical information is increasing with the fusion of PHR technology and healthcare. In this paper, therefore, we analyze the various security aspects that are vulnerable to the PHR service and needed to be resolved. Moreover, we analyze the security requirements from the point of view of the PHR users and application service providers and provides the PHR security mechanism for addressing PHR security threats and satisfying PHR security requirements.

Key Words : PHR, personal health record, security, privacy, healthcare

Ⅰ. 서 론

최근 정보통신기술의 발전과 고령화, 국민의 소득증대 등의 영향으로 u-헬스케어 산업이 급성장세를 보이고 있으며, IT 기술을 의료 분야에 다양한 형태로 융합하여 국민 건강과 삶의 질을 높일 수 있는 u-헬스케어 서비스에 대한 연구가 활발하게 진행되고 있다. u-헬스케어는 스마트폰이나 가정용 생체정보 측정기기를 이용하여 가정 내에서 건강과 관련된 각종 생체정보를 측정하고 이를 인터넷을 이용해 헬스케어 서비스 센터로 전송하여, 건강상태를 지속적으로 모니터링함으로써 질병을 관리하고 응급상황을 대비할 수 있는 서비스이다. u-헬스케어는 병원이라는 물리적 공간에서만 진단, 치료, 관리가 이뤄지던 의료서비스가 조만간 가정에서 사무실에서 이동

*정회원, 가천대학교 IT대학 컴퓨터공학과
**정회원, 가천대학교 IT대학 컴퓨터공학과(교신저자)
접수일자: 2015년 10월 15일, 수정완료: 2015년 11월 15일
게재확정일자: 2015년 12월 11일

Received: 15 October, 2015 / Revised: 15 November, 2015 / Accepted: 11 December, 2015
**Corresponding Author: hwanghj@gachon.ac.kr
Dept. of Computer Engineering, Gachon University, KOREA

중에도 언제 어디서라도 인터넷과 모바일 기술에 접목된 각종 유비쿼터스 의료기기를 통해 환자와 병원이 연결되는 시대를 맞게 될 것으로 전망하고 있다. 최근 u-헬스케어 영역은 환자의 단순한 질병의 치료에서 예방으로 이동하는 추세에 있으며 병원의 공공의료 중심에서 환자 중심으로 패러다임이 변화하고 있다. 병원내의 전자의무기록(Electronic Medical Record, 이하 EMR) 시스템 외에 환자가 가정 및 일상에서 이용할 시스템이 필요하게 되었다. 개인건강기록(Personal Health record, 이하 PHR)은 ' 다양한 의료기관으로 부터 제공되는 개인의 진료정보와 개인 스스로 기록한 건강기록을 통합적이고 포괄적인 관점에서 바라본 개인의 평생건강기록과 그 기록을 관리할 수 있는 도구'를 말한다[1]. 개인 건강에 관한 데이터와 문서를 원하는 시간과 장소에 환자나 보호자, 의료진과 같은 관련자들 사이에 효율적으로 접근하고 공유하며, 건강관리의 안전성과 품질을 높이고 치료의 효율을 향상시키는데 있다. PHR과 EMR의 주요 차이점은 EMR의 경우 정보의 통제권이 의사나 병원에게 있지만, PHR은 정보의 통제권이 개인에게 있다는 점이다. EMR은 디지털 형식의 개인의 의료 기록을 의미한다. EMR은 병원정보시스템을 사용하여 개인의 건강 기록을 저장하고 이용하며, 환자의 신상명세, 치료기록, 약품 및 알레르기 목록, 면역상태, 검사결과, X-레이나 MRI와 같은 영상 사진, 보험기록 및 세부 지시 사항 등을 포함한다. PHR은 개인이 건강에 관한 여러 가지 결정을 내리는 데 활용할 수 있으며 언제 어디서나 평생 사용할 수 있는 건강 정보 자원이다. PHR은 헬스케어 서비스 제공업체와 개인이 제공한 PHR에서 자신의 정보를 소유하고 관리한다. PHR은 여러 가지 장점을 가지고 있다. 먼저, PHR를 통해 환자는 신뢰할 수 있는 개인의 건강정보에 대한 접근이 용이해지며, 환자 스스로 자신의 건강이력 및 병력 등을 관리하게 함으로써 평생 지속적인 건강 및 치료를 가능케 한다. 또한, 환자의 보호자에게 올바른 환자 관리 정보를 제공할 수 있다. 또한, 의료진은 환자로부터 더 많은 데이터를 제공받음으로서 더 나은 진단 및 처방 의사결정 가능하고, 의료정보 제공자간의 간접적인 진료정보공유 방법을 제공할 수 있으며, 기존 환자와의 상담 형태보다 객관적이고 정확하며, 효과적인 소통 방법 제공한다.

PHR를 활용한 대표적인 서비스를 살펴보면 다음과 같다. 미국 CMS(Centers for Medicare and medicaid Services)는 'Meaningful Use' 프로그램을 제시하여 2016년까지 단계적으로 EMR의 의료 자료 공유 활성화를 추진하고 있다. 1단계에서는 정부기관에서 인센티브를 부여하여 의사들의 적극적인 참여를 통해 전자적 의료 자료를 축적하였으며, 2단계에서는 사용자들의 자료 이용률을 높이도록 추진 중이다. 마지막으로 3단계에서는 자동적으로 의료정보가 공유되고 예후 정보까지 포함되도록 환자 중심의 향상된 의료서비스를 추진할 예정이다. 이러한 Meaningful Use 프로그램의 의료데이터 공유 방식으로 아이블루버튼(iBlue Button)이 활용되고 있다. 아이블루버튼은 65세 이상 또는 소정의 자격 요건을 갖춘 사람에게 제공하는 건강보험인 메디케어 기록을 열람할 수 있는 앱이다. 아이블루버튼은 자신이 어떤 진단을 받았고, 어느 병원과 응급실에서 어느 의사에게 진료를 받았으며, 엑스레이와 처방, 건강검진을 언제 어디에서 받았는지 상세히 알려준다. 다른 소스로 연결되는 링크를 타고 가면 환자와 가족, 의료진이 질환과 약력까지 찾아볼 수 있다. 또한, 환자들은 '아이블루버튼 프로페셔널'을 다운로드한 의사들에게 자신의 메디케어 기록을 전송할 수도 있다. 애플의 경우 아이폰의 운영체제인 iOS8 부터 헬스키트(HealthKit)라는 플랫폼을 기본적으로 탑재하고 있다[2]. 사용자들은 이 하나의 플랫폼 안에서 각종 헬스케어 웨러러블 디바이스, 앱들을 사용하여 심박수 및 혈압을 모니터하고 포도당 센서, 건강 온도계 등과 같이 측정한 건강 및 의료 데이터를 열람할 수 있도록 소프트웨어 측면에서 지원하게 된다. 또한, 에픽 시스템즈(Epic Systems) 등의 대형 EMR 기업과의 협업을 통해서 병원까지 그 데이터를 보낼 수 있다. 애플은 iOS 8의 헬스킷(HealthKit) 툴을 테스트하기 위한 건강 관리 서비스 업체와 공조하고 있으며, 스탠포드대학병원과 듀크대학병원이 헬스킷의 임상 테스트에 참여하고 있다. 듀크대학병원 의사들은 심장 질환과 암 환자의 혈압 등 생체 정보를 모니터링할 예정이며 스탠포드대학병원 의사들은 소아 당뇨를 앓고 있는 어린이들의 혈당을 추적하는데 헬스킷를 사용하고 있다. 마이크로소프트는 클라우드 기반의 '마이크로소프트 헬스(MicroSoft Health, 이하 MS 헬스)' 서비스를 통해 헬스케어 시장을 바꾸고 있다[3]. MS 헬스는 웨어러블 기기나 앱에서 수집된 데이터를 기반으로 새로운 통찰을 제공해 더 건강한 생활을 돕는 것이 목표이다. MS는 MS 헬스를 개방형 플랫폼으로 운영해 활동, 영양상태, 운동과 휴식 등에 대한 다양한 정보가 모일 수 있도록 하고 있다. 또한, 매일 섭취 칼로리, 운동량, 질

병 등을 체크하고, 음식, 운동, 의료정보를 얻을 수 있는 'MSN건강' 앱도 서비스하고 있는데, MS 헬스와 연결돼 머신러닝 기반의 학습능력을 갖고 있다. 머신러닝을 이용하면 평상시 심장박동과 비교해 적절한 운동량 등을 판단하고 조언한다. MS는 개인의 건강정보를 수집할 수 있는 웨어러블 디바이스인 'MS 밴드[4]'도 출시했다. MS 헬스, MSN 건강과 연동되는 MS 밴드는 열 가지 센서를 이용해 사용자의 심박 수, 수면의 질, 체온, 보행거리, 자외선 노출정도 등을 측정할 수 있다. MS 헬스, MSN 건강, MS 밴드 등을 통해 수집된 정보는 '헬스볼트[5]'에서 통합관리 되며 개인이 등록할 수 있는 일상적인 건강정보는 물론 병원, 약국 등의 정보까지 저장, 관리할 수 있다. MS는 병원과 연계해 헬스볼트에 저장된 의료정보가 진료 등 의료 서비스에 사용될 수 있도록 하고 있다. 위에서 살펴본 바와 같이 PHR 서비스 경우 많은 양의 매우 민감한 사용자 데이터를 관리하기 때문에 새로운 기술에 대한 보안이 매우 중요하다. 환자, 보호자, 병원과 같은 PHR 주체와 정보 전송 및 저장과정에서 발생할 수 있는 위·변조, 외부의 침입, 바이러스 감염 등 다양한 보안위협들이 존재하며 PHR 데이터 저장 및 전송과 관련된 프라이버시 및 보안 문제해결이 반드시 선행되어야 한다. 본 논문에서는 PHR 보안의 위협요소를 살펴보고 PHR 보안기술의 동향을 분석한다.

본 논문의 구성은 다음과 같다. 2장은 PHR 서비스에서 발생할 수 있는 보안 위협요소에 대해서 분석하고, 3장은 안전한 PHR 서비스를 위한 보안 요구사항에 대해서 분석한다. 4장은 PHR 서비스 보안위협에 대응하기 위한 보안 기술을 분석하고, 5장은 결론을 도출한다.

II. PHR 보안 위협요소

본 장에서는 PHR 서비스 보안 위협요소에 대해서 분석하고자한다. 컴퓨팅 환경은 클라이언트-서버 기반의 유선 네트워크에서 각종 사물에 센서와 통신 기능을 내장하여 유선 뿐 아니라 무선을 통해 인터넷에 연결하는 사물 인터넷 환경으로 변화하고 있다. 단순히 개인용 컴퓨터 뿐 아니라, 노트북, 스마트폰, 테블릿 PC와 같은 다양한 형태의 휴대가능한 장비들을 이용하여 PHR를 전송하고 있으며, 이러한 다양성과 휴대성은 보안 취약성을 더욱 심화시키고 있다. 누구나 쉽게 접근이 가능하고 휴대가 가능한 단말의 특성은 개인의 사생활 정보를 보호하기 어렵게 만들고, 무선 통신의 특성상 데이터의 가로채기 등을 통해 위·변조가 가능하기 때문에 중요한 PHR 데이터에 대한 보안이 더욱 어려워지고 있다. 대부분의 휴대형 장비들은 휴대성을 위해서 면적, 소비전력의 최소화를 요구하기 때문에 보안 모듈이 없거나 다소 약한 수준의 보안 모듈이 제공되고 있다. PHR 환경에서 발생할 수 있는 보안의 위협들은 기존의 정보통신환경에서 발생할 수 있는 보안 위협요소를 상속한다. 즉, 기존의 IT분야에서 존재하는 보안 취약성이 PHR 서비스 환경에서도 그대로 존재하며, 심지어는 기본 위협보다 더 심각한 경우도 있다. 일반적으로 정보보안의 목적을 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 등을 유지하는 것이라 정의하며 이러한 속성을 저해하는 행위를 보안위협이라고 할 수 있다. PHR 서비스를 이용함에 있어서 보안적인 측면에서 우려되는 문제점으로는 보안 및 데이터 유출, 프라이버시 침해, 서비스 안정성 등을 들 수 있다. 개인의 신원이나 생체정보, 개인정보와 같은 민감 데이터가 암호화되지 않고 평문으로 전송되는 경우 개인정보 유출의 심각한 문제가 발생하게 된다. 또한, PHR 서비스 주체간의 PHR 데이터를 교환하는 경우 데이터를 중간에 가로채어 위조 및 변조를 통해 인가된 사용자처럼 위장할 수 있는 위협이 존재한다. PHR 서비스의 경우 수집된 개인건강 정보를 자신의 개인 저장소인 클라우드나 서버에 주기적으로 전송해야하는 관계로 공격자는 이러한 특성을 악용하여 임의의 대량연결 요청이나 서비스 확인 패킷을 지속적으로 전송하여 단말 및 서버의 가용한 자원을 소모시키고 정상적인 서비스가 불가능할 수 있도록 유도가 가능하다. PHR 서비스에서 가능한 핵심 보안 위협을 정리해보면 표 1.과 같다.

표 1. PHR 서비스의 보안 위협
Table 1. Security Threats for PHR services

구분	보안 위협요소
단말 및 서버	악성코드 감염 및 확산, 웜(Worm)과 바이러스, 악의적인 펌웨어, 단말기 분실로 인한 정보유출, 패치되지 않은 시스템 운영체제, OS 보안의 취약성, 방화벽 오류 및 잘못된 정책
네트워크	비인가된 접근, 프로토콜의 취약성, 서비스 거부, DDoS, 무결성 오류, 데이터의 가로채기, 데이터의 위변조,
응용프로그램 및 서비스	안전하지 않은 패스워드, 비인가된 사용자의 접근, 버퍼 오버플로우, 프라이버시 침해, 시스템 장애, 서비스 거부

표 1에서 언급한 보안 취약성 뿐 아니라 PHR 데이터를 부적절하게 이용될 경우 개인의 프라이버시 침해로 이어질 수 있다. PHR 데이터를 안전하게 활용하고 공유하기 위한 기술적 보안 및 프라이버시 보호 장치가 마련되어야 한다. PHR 데이터는 원칙적으로 개인의 건강관리를 목적과 의료진과 보호자 등의 속성을 고려하여 사용범위를 설정되어야 한다. 연구목적이나 다른 환자의 치료를 목적으로 하는 경우 개인의 사전 동의가 필요하며, 이러한 경우 개인정보는 익명화되어서 사용해야 하는 조건이 필요하다. 개인의 프라이버시 보호를 위하여 PHR 데이터를 접근하는 사람에 대한 기밀성 유지가 필요하며 PHR 서비스 내역 및 서비스 사용자에 대한 프라이버시 보호와 권한관리 유지가 필요하다.

Ⅲ. PHR 보안 요구사항

본 장에서는 PHR 서비스 보안 요구사항에 대하여 분석하고자한다. PHR 서비스의 구성요소는 서비스 특성에 따라 다양하지만 단말와 서버, 네트워크, 어플리케이션 및 서비스로 구별할 수 있다. PHR 서비스를 위한 단말의 경우 CPU 성능, 메모리 크기, 소비전력의 제약을 가지고 있어서 단말의 특성 및 보안강도를 고려한 보안 기술을 요구하게 된다. PHR 서비스에서 필요한 보안 요구사항의 주요내용을 정리하면 표 2와 같다.

표 2. PHR 서비스의 보안 요구사항
Table 2. Security Requirement for PHR services

구분	보안 위협요소
단말 및 서버	권한설정, 인증, 무결성, 접근통제, 데이터의 암호화 및 복호화
네트워크	프로토콜의 접근제어 권한 설정, 인증, 데이터의 기밀성 및 무결성, 네트워크 보안, 암호화 및 복호화
응용프로그램 및 서비스	서비스의 권한 설정, 사용자 인증과 접근제어, 데이터의 기밀성 및 무결성, 프라이버시 보장, 보안감사, 백업 및 복구, 부인방지

환자, 보호자, 병원 의료진과 같은 PHR 서비스 주체 사이에 전송되는 모든 데이터는 비 인가된 접속, 비 인가된 수정 또는 비 인가된 사용자로부터 보호되어야 한다. 기밀성 보호를 위해 기본적인 사용자 식별을 위한 사용자 인증, 키 관리, 암호화 및 복호화의 보안 기술이 제공되어야 하며 단말의 특성을 고려하여 경량화 된 키 분배 및 보안 알고리즘이 적용되어야 한다. PHR 주체간의 교환을 위하여 저장되는 데이터와 메시지에 대한 오류검사가 필요하며 무결성이 보존되어야 한다. 또한, 서비스 중단이나 데이터 손실을 막기 위한 백업 및 복구가 필요하고 효과적인 보안을 위해 사용자별 권한 관리 및 사용내역이 감사기록으로 관리되어야 하며, 병원 및 건강관리 기관과 서비스 상호 연동을 위하여 PHR을 보호하기 위한 접근제어 정책 및 절차를 수립하고 적용하여야 한다. 무선을 통한 연결은 보안성이 검증된 인증방식을 사용하여야 하며, 허가되지 않은 무선연결은 제한하여야 한다.

또한, 개인정보 유출로 인한 프라이버시 침해를 방지할 수 있는 방법이 제공되어야 한다. 미국의 경우 의료정보보호법(Health Insurance Portability and Accountability Act, 이하 HIPAA)[6]에서는 개인 건강정보의 사용과 노출은 물론 개인이 자신의 건강정보가 어떻게 사용되는지 알고 이를 통제할 수 있는 프라이버시 권리를 위한 표준에 대하여 규정하고 있다. 또한, 이름, 사회보장번호, 병록번호 등 18개 항목을 민감 건강정보(Protected Health Information, 이하 PHI)로 규정하고, 임상자료 연구 활용의 기본조건으로 민감 건강정보에 대한 익명화를 규정하고 있다. 또한, 개인 식별정보 제거를 위한 구체적인 방법으로 개인 식별정보를 삭제하거나 사회적 차별의 가능성이 있는 민감한 진단명 삭제, 일정한 범위 내에서 환자의 모든 날짜정보 동시 이동 등의 방법을 제시하고 있다.

또한, OECD 정보보안 및 프라이버시 워킹그룹(Working Party on Information Security and Privacy, 이하 WPISP)은 프라이버시 가이드라인 개정에 대한 검토 합의안(Terms of Reference, TOR)을 2011년에 도출하였으며, 2013년 7월 11일 OECD 이사회는 프라이버시 보호 및 개인 데이터의 국경 간 유통에 관한 가이드라인(Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)의 개정안 권고문을 채택하였다. 이 가이드라인은 프라이버시 관리 프로그램을 도입하고 프라이버시 집행기관을 설립, 개인정보 관리에 대한 역할과 책임을 강화하는 것이 주요 골자이며, 데이터 보안에 기여하고 정보관리자의 책임성 강화를 위해 '개인정보 유출의 통지 및 신고'제도를 도입했다. 또한 워킹그룹은 OECD 프라이버시 프레임워크에 프라이버시 관리 프로

그램, 보안 유출 통지, 국가 프라이버시 전략, 교육과 의식, 그리고 글로벌 상호 운용성 등 몇 가지 새로운 개념을 도입하였다. 표 3과 같이 OECD WPISP에서 제시한 8개의 원칙은 개인정보의 수집 및 관리에 대한 국제사회의 합의를 반영한 국제기준으로 법적인 구속력은 없지만 개인정보보호의 일반 원칙으로 인정받고 있다.

표 3. OECD 프라이버시 가이드라인
Table 3. OECD privacy guideline

보호원칙	내용
수집제한	개인정보의 수집은 원칙적으로 제한돼야 하고 어떤 개인정보도 합법적이고 정당한 절차에 의해 수집돼야 하며, 경우에 따라 정보주체에게 통지하거나 동의를 얻어야 함
정보 정확성	개인정보는 그 이용목적에 부합되는 것이어야 하고 이용목적상 필요한 범위 내에서 정확하고 완전하며 최신의 것으로 보존되어야 함
목적 구체성	개인정보의 수집목적은 수집할 당시 미리 특정돼 있어야 하고 차후의 이용은 구체화된 목적의 달성과 일치돼야 하며, 수집목적이 변경될 때마다 그 목적을 명확하게 해야 함
사용 제한	개인정보가 목적 구체성의 원칙에 의하여 명시된 목적 이외의 다른 목적을 위해 공개, 이용, 기타 사용에 제공돼선 안됨
안전성 확보	개인정보는 분실 또는 부당한 접근, 파괴, 수용, 수정, 공개 등의 위험으로부터 적절한 안전성 확보장치에 의해 보호되어야 함
공개	개인정보 처리와 관련된 정보처리장치의 개발, 활용, 정책은 일반에게 공개되어야 함
개인참여	개인이 정보관리자로부터 자신과 관련된 자료를 얻거나 그 밖에 자신에 대한 정보의 소재를 확인할 권리를 가짐
책임	모든 원칙이 지켜지도록 필요한 조치를 취할 책임이 있음

그 외 프라이버시 침해를 막기 위하여 UN 개인정보파일의 전산화에 관한 가이드라인(Un Guidelines Concerning Computerized Personal Data Files, 1990), EU 개인정보보호에 관한 유럽연합지침(The Protection of Individuals with regard to the Procession of Personal Data and on the Free movement of such Data, 1995), ILO 근로자의 개인정보보호규약(ILO Code of Practice on the Protection of Worker's Personal Data, 1997), 호주의 민간의료분야에서의 프라이버시에 관한 가이드라인(Guidelines on Privacy in the Private Health Sector) 등이 제공되고 있다. 국내의 경우 개인의료정보 관련 정책의 필요성은 수차례 제기 되어 왔으나 의료법 및 보건의료관련 법률에 프라이버시가 보장되어 있지 않다. 국내의 경우 개인정보보호 관련 법제는 공공분야와 민간분야로 분리하여 운영 중이며, 공공분야는 공공 기관의 개인정보보호에 관한 법률에 의해서 규율하고 있고, 민간분야는 정보통신망이용촉진 및 정보보호 등에 관한 법률에서 개인정보에 대한 전반적인 사항을 규율하고 있다. 또한 의료법 제19조(비밀누설의 금지), 제20조(진료기록 등), 제21조 2항(전자의무기록), 결핵예방법, 정신보건법, 국민건강증진법, 전염병예방법, 약사법 등의 개별 법령에서 진료정보 기밀누설을 금지하고 있으나 환자 개인의료정보보호를 위한 종합적인 규정이 없어 정보보호에 한계가 있다.

Ⅳ. PHR 보안기술

본 장에서는 안전한 PHR 서비스 제공을 위한 경량알고리즘 및 기타 보안 기술 동향에 대해 기술하고자 한다. PHR 서비스 제공을 위한 단말의 경우 매우 제한적인 연산속도와 저장 공간을 소유하고 있어서 가지고 경량화된 암호 알고리즘이 필수적이다. 본 장에서는 경량 암호알고리즘 및 PHR 서비스를 위한 주요 보안기술에 대해서 분석한다.

1. AES 알고리즘

AES(Advanced Encryption Standard)암호는 미국 표준 기술 연구소(NIST)가 DES를 대체할 목적으로 알호기법 공모를 통해 선정된 알고리즘으로 두 명의 벨기에 학자인 Joan Deamon과 Vincent Rijndael이 개발한 암호이다. AES는 DES의 Feistel 구조와 달리 대체(substitution)와 치환(permutation)을 반복 적용하는 SPN(Substitution - Permutation Network)구조를 이용하며 128비트와 256비트의 키 길이를 선택할 수 있다. AES의 암호화 과정의 각 라운드는 함수의 값이 독립변수의 값과 비례관계에 있지 않는 비선형성을 갖는 S-BOX를 적용하여 바이트 단위로 치환을 수행하는 연산, 행 단위로 순환 시프트를 수행하는 연산, 높은 확산(diffusion)을 제공하기 위해 열 단위로 혼합하는 연산, 라운드 키 값을 현재의 평문과 XOR하는 연산으로 구성되어있다.

2. HIGHT

HIGHT(HIGh security and light weigHT)암호는 센서 네트워크와 같은 저전력, 경량화를 요구하는 컴퓨팅 환경에서 기밀성을 제공하기 위한 목적으로 개발된 64비트 블록 암호 알고리즘이다[7]. 2010년 ISO/IEC 국제표준으로 채택되었으며 128비트 마스터키, 64비트 평문으로부터 64비트 암호문을 출력한다. 자원의 제약성을 고려하여 8비트 단위의 기본적인 산술 연산들인 XOR, 덧셈, 순환이동만으로 설계되었다. HIGHT는 SEED, AES등 기타 알고리즘보다 간단한 알고리즘 구조로 설계되었으며, 일반화된 Feistel 변형 구조로 이루어져 있다. 64비트의 평문을 사용하며 128비트 마스터키로부터 생성된 8개의 8비트 화이트닝 키와 128개의 8비트 서브키를 입력으로 사용하여 32개의 라운드 연산을 한다. 그리고 마지막 최종변환을 한 후 64비트의 암호문을 출력한다.

3. ARIA

ARIA 암호는 경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조의 범용블록 암호 알고리즘이다[8]. 블록 크기는 128비트를 사용하며, AES 암호와 동일한 128비트, 192비트, 256비트의 길이의 키를 사용한다. 키 크기에 따라, 12라운드, 14라운드, 16라운드를 각각 수행하며 사용하는 대부분의 연산은 XOR과 같은 단순한 바이트 단위 연산으로 구성되어 있다. ARIA 블록 암호의 입력과 출력은 각각 128비트들의 수열로 구성되며, 기본 연산 단위는 바이트로 입력 및 출력과 암호 키의 비트 수열은 연속된 8바이트로 묶은 바이트 배열로 처리된다.

3. CLEFIA

SONY에서 개발한 AES와 유사한 형태의 블록암호 알고리즘으로 128비트의 평문사용하며, AES 암호와 동일하게 128비트, 192비트, 256비트 길이의 키를 사용할 수 있다[9]. 전통적인 2개의 데이터 라인으로 구성된 Feistel 구조와 달리 그림 1와 같이 4개의 데이터 라인으로 구성된 Feistel 구조로 되어 있으며, 각 라운드마다 2개의 F함수를 사용한다. 한 라운드마다 F함수는 병렬적으로 위치하며, 32비트 길이의 입력과 출력으로 연산된다.

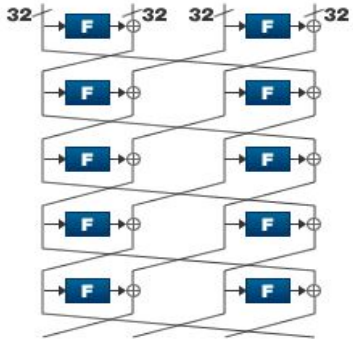

그림 1. CLEFIA의 구조
Fig. 1. CLEFIA architecture

4. LEA

LEA(Lightweight Encryption Algorithm)암호는 국가보안기술연구소에서 개발하였으며 128비트의 경량 블록 알고리즘으로 사용목적에 따라 128비트, 192비트, 또는 256비트의 키 사용이 가능하다[10]. AES나 DES와 같은 S-BOX를 사용하지 않고, 비트수준의 ARX(Addition, Rotation, Xor) 연산만으로 구성하여 동작하도록 설계되었으며, AES의 연산속도보다 빠르고 훨씬 적은 메모리 공간을 차지한다.

5. PRESENT

PRESENT 암호는 AES를 기반으로 하며 31라운드 SPN 구조로 되어있으며, 64비트 블록 암호로서 80비트나 128비트 길이의 키를 사용하며 매우 제한적인 컴퓨팅 자원 적합하도록 설계되었다[11]. 전체구조는 4비트의 S-BOX와 XOR 및 비트 시프트로 연산으로 구성되어 있고, 암호학 강도는 AES에 비하여 떨어지지만 면적과 소비전력을 개선시킨 암호 알고리즘이다.

6. SEA

SEA(Simple Encryption Algorithm)암호는 파일 암호화와 실시간 스트리밍을 지원하는 매우 단순한 보안 알고리즘이다[12]. 데이터블록의 크기 및 키의 길이를 암호화 강도 및 계산비용에 따라 가변적으로 조정이 가능하며, 소프트웨어로 구현이 쉽고 데이터와 키의 비트수에 따라 라운드 및 워드의 크기가 달라지는 유연함을 가지고 있다. 암호화 및 복호화 연산이 동일하며, 하나의 메인 키로부터 파생된 서브키를 이용하여 유사 일회용 암호를

생성하여 암호화에 이용한다. 특정특정 알고리즘에 의존하지 않아 SHA-160같은 Secure Hash Algorithm이나 Cipher Algorithm을 선별적으로 사용할 수 있다. 다양한 확장성 기본 원리가 매우 단순하고 파일 암호화 및 스트림 통신 등의 모든 방식으로의 응용 및 확장 개발이 용이하다.

7. TEA와 XTEA

TEA(Tiny Encryption Algorithm)는 David J. Wheeler와 R. Needham에 의해 소개되었으며 적은 전력 소모와 빠른 속도를 목적으로 설계되었다[13]. TEA는 간단한 키 스케줄을 사용하는데, 이로 인해 연관키 공격이 가능하였다. 설계자들은 이런 약점들을 보완하여 XTEA(TEA Extensions)를 다시 제안하였다. XTEA는 TEA와 마찬가지로 XOR, 시프트, ADD와 같은 기본적인 산술 및 논리 연산들을 사용하여 설계되었으며 Feistel 구조의 32라운드를 진행하는 동안 키는 변형되지 않으며 62비트의 평문과 128비트의 키를 사용한다.

8. Hummingbird와 Hummingbird-2

Hummingbird 암호는 Revere Security사에서 개발한 경량 알고리즘이다[14]. 256비트의 키 사이즈, 16비트의 메시지 블록 길이를 가지는 대칭키 알고리즘이며, 전력소모가 작고 적은 면적을 요구하며 우수한 성능을 보여준다. 하지만, 차분 공격에 대한 취약성으로 인해 이를 보안한 Hummingbird-2 알고리즘이 제안되었다. 제안하였다. Hummingbird-2 알고리즘은 128비트의 키와 16비트의 평문 블록을 입력받아 16비트의 암호문 블록을 출력한다.

9. DES-X

DES-X는 DES의 변형 알고리즘으로 S-BOX를 새롭게 설계하여 선형분석(linear cryptanalysis)과 차분공격(differential cryptanalysis)등에 대항하기 위한 키 화이트닝(Key Whitening) 기법을 사용하여 무작위 공격의 복잡성을 증가시킨 대칭형 블록 알고리즘이다. DES와 동일하게 64비트의 평문을 암호화 하고, 196비트의 키를 사용한다. DES와 차이점이 있다면 S-BOX로 단일화하여 경량화함으로써 전체 크기를 감소시켰다.

10. mCRYTON

CRYPTON 알고리즘을 기반으로 제한된 컴퓨팅 자원을 위해 설계되었으며 64비트의 블록평문과 64비트, 96비트, 128비트의 길이의 키를 사용할 수 있다[15]. Feistel 구조로 12 라운드로 구성되며 차분공격과 선형 공격 등에 충분한 안전성을 가지고 있는 것으로 평가된다.

11. 기타 PHR 보안 기술

앞에서 분석한 다양한 경량 알고리즘을 기반으로 각 서비스 계층에서 기존의 인터넷 보안기술을 적용이 가능하다. 웹 서비스의 경우는 W3C에서 제안한 XML[16,17] Signature/Encryption, XKMS 2.0, SOAP-SEC와 OASIS에서 제안한 SAML, XACML 등을 활용하여 XML 형태의 PHR 문서 보안에 활용이 가능하다. 또한, PHR 서비스 사용자의 단말과 서버 사이의 보안은 SSL(Secure Sockets Layer), TLS(Transport Layer Securit), WTLS(Wireless Transport Layer Security), AnyWeb의 MMS(Mobile Micro Security) 등과 같은 보안 프로토콜의 적용이 가능하다. 근거리 서비스의 경우 IEEE 802.15.4에 보안 기술에서 제공하는 접근제어 리스트, 데이터 암호화, 프레임 무결성 기능을 활용할 수 있으며, Zigbee 프로토콜에서 제공하는 ZDO(ZigBee Device Object)의 보안 기술, CoAP(Constrained Application Protocol)과 MQTT(Message Queuing Telemetry Transport) 프로토콜을 활용하여 보안을 향상시킬 수 있다.

V. 결 론

최근 언제 어디서나 건강 증진 콘텐츠를 제공하고 건강관리 서비스를 제공하기 위한 PHR 서비스에 대한 연구가 활발히 진행되고 있으며, PHR 서비스의 활성화를 위해서 보안이 필수적인 요소가 되고 있다. 본 논문에서는 PHR 서비스에서 발생할 수 있는 다양한 보안위협요소를 분석하고 보안요구사항을 도출하였으며, 이를 바탕으로 적용할 수 있는 경량화 된 보안 알고리즘 및 적용할 수 있는 보안 기술을 분석하였다. 안전한 PHR 서비스 제공을 위해서 본 논문에서 기술한 보안위협요소와 분석한 보안기술을 바탕으로 대응방안을 마련해야 할 것이다.

References

[1] Yuksel, M., Dogac, A."Interoperability of Medical Device Information and the Clinical Applications: An HL7 RMIM based on the ISO/IEEE 11073 DIM", , IEEE Transactions on Information Technology in Biomedicine, Volume 15, Issue 4, Pages: 557 - 566, 2011

[2] https://developer.apple.com/healthkit/

[3] https://www.microsoft.com/microsoft-health

[4] http://www.microsoft.com/microsoft-band/

[5] https://www.healthvault.com/

[6] Personal Health Records and the HIPAA Privacy Rule.

[7] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, Seongtaek CheeShow less, "HIGHT: A New Block Cipher Suitable for Low-Resource Device", Lecture Notes in Computer Science, Vol. 4249, pp 46-59, 2006.

[8] JeaHoon Park, JaeCheol Ha, "Improved Differential Fault Analysis on Block Cipher ARIA," Lecture Notes in Computer Science, Vol. 7690, pp 82-95, 2012.

[9] Hamid Mala , Mohammad Dakhilalian, Mohsen Shakiba, "Impossible Differential Attacks on 13-Round CLEFIA-128", Journal of Computer Science and Technology, Volume 26, Issue 4, pp 744-750, July 2011.

[10] Hong, Deukjo, Jung-Keun Lee, Dong-Chan Kim,Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee. "LEA: A 128-bit block cipher for fast encryption on common processors." In Information Security Applications, pp. 3-27. Springer International Publishing, 2014.

[11] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", Lecture Notes in Computer Science, Volume 4727, pp 450-466, 2007.

[12] Elena Trichina, Domenico De Seta, and Lucia Germani, "Simplified Adaptive Multiplicative Masking for AES", Lecture Notes in Computer Science(LNCE), Vol.2523, pp.71~85, 2003.

[13] Wheeler, David J. and Needham, Roger M. "TEA Extensions". Computer Laboratory, Cambridge University, England. October, 1997.

[14] ENGELS, Daniel, et al. The Hummingbird-2 lightweight authenticated encryption algorithm. In: RFID. Security and Privacy. Springer Berlin Heidelberg, 2012. p. 19-31.

[15] Eunjong Hong, Jai-Hoon Chung, Chae Hoon Lim, "Hardware Design and Performance Estimation of the 128-bit Block Cipher Crypton", Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems, Pages 49-60, 1999.

[16] Myung-Kyu Yi, Hee-Joung Hwang, "A Low Power Lifelog Management Scheme Based on User Movement Behaviors in Wireless Networks" The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 15, No. 2, pp.157-165, Apr. 30, 2015.

[17] Yun-Jeong Lee, Hyung-Deok Shin, "Effects of Contents Narrativity on the Related Contents Preference: Surveying on Korean College Students", Journal of the Korea Academia-Industrial cooperation Society, Vol. 16, No. 1 pp. 62-69, 2015

저자 소개

이 명 규(정회원)

- 2005년 2월 : 고려대학교 컴퓨터학과 (이학박사)
- 2006년 10월 ~ 현재 : 가천대학교 IT 대학 컴퓨터공학과 연구교수
- TTA 유헬스 프로젝트그룹 개인건강정보 표준화 전담반 위원

<주관심분야 : u-Health, Big Data, Medical Informatics, Security, Ubiquious Computing>

황 희 정(정회원)

- 2000년 9월 : 인하대학교 컴퓨터공학과(공학석사)
- 2008년 2월 : 인천대학교 컴퓨터공학과(공학박사)
- 2000년 10월 ~ 현재 : 가천대학교 IT대학 컴퓨터공학과

<주관심분야 : Software Engineering, u-Health, Big Data,Medical Informatics, Ubiquious Computing>

※ 이 논문은 2015년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 [B0101-15-247 개인 건강정보 기반 개방형 ICT 힐링 플랫폼 기술 개발]