XML 기반 PHI를 휴대하기 위한 프라이버시 보안

Privacy Security for Carrying XML-based Personal Health Information

Hyo Jung Seo, Dae Wook Bang PhD†, Yoon Nyun Kim PhD††, Kyung Il Youn PhD††,

Myoung Hwa Park PhD†††

* Department of Computer Engineering, Graduate School, Keimyung University, Daegu 704-701, hjseo@kmu.ac.kr
† Department of Computer Engineering, College of Information and Communication, Keimyung University, Daegu 704-701
††Department of Medical Information, College of Medicine, Keimyung University, Daegu 700-712
†††Department of Nursing, College of Nursing, Keimyung University, Daegu 700-712

Abstract: The purpose of this study was to design a specification of privacy security for a XML-based PHI, MyPHR. MyPHR document has a root element, MyPhr, with two child elements, MyPhrHeader and MyPhrBody. MyPhrHeader element has management information of itself, and MyPhrBody element includes one or more MyPhrModules which represent their own type of health record. MyPHR guarantees privacy security through access control and encryption specification that can be processed only by its management system. It has elements representing access control lists within MyPhr document and permits to encrypt elements representing private information by using XML Encryption. Private information of MyPHR document is included within both protectedInfo element of MyPhrHeader and MyPhtBody element. This study identified that privacy security is guaranteed by two security mechanisms, encryption and access control. Encryption hides private information from all persons excepting the person who has the security key, and access control protects unauthorized access of private information.

Keyword: *personal health record, privacy security, encryption, access control*

I. 배 경

PHI(Personal Health Information)란 개인이 직접 입력하고 관리할 수 있는 일종의 PHR(Personal Health Record)이다.[1,2] 현재 ISO/TC215, DICOM, HL7, ASTM, MedXML 등의 표준기관에서 EHR(Electronic Health Record)의 한 범주로 표준 PHR 사양을 제정하고 있으며, 미국건강정보관리협회(AHIMA: American Health Information Management Association)는 PHR 소개 사이트(www.myPHR.com)에서 현재 운영되고 있는 PHI 서비스 사이트들을 링크하고 있다.

일반적으로 PHI는 문서 파일로 저장되거나 데이터베이스 레코드로 저장된다. 데이터베이스 레코드는 웹 서버에 보관되고 웹 서비스를 통해 개인이 접근할 수 있다. 반면에 문서 파일은 웹 서버에 보관하고 사용할 수도 있고, 개인이 휴대하는 PDA, 휴대전화, 스마트 카드 등의 휴대 저장장치에 담아서 사용할 수도 있다.

PHI가 언제 어디서나 개인을 위해 활용되게 하려면 개인이 휴대하여야 한다. 개인이 휴대하려면 PHI는 서버 저장소에서 휴대 저장장치에 복사되어야 한다. 그 결과 복사된 PHI가 어떠한 환경에서도 저장소에 있는 원본과 동일함을 보장하여야 하고, PHI가 시중에 유통되어도 개인 프라이버시가 침해되지 않도록 프라이버시 보안이 보장되어야 한다. 본 연구는 이러한 휴대를 위한 필요조건 중에서 서버 저장소에서 복사하여 휴대하여도 프라이버시 보안을 보장할 수 있는 XML 기반 PHI의 보안 스펙을 제안하고 검증한다.

II. 방 법

본 연구는 의료기관의 의무기록 중에서 개인이 평생 관리할 필요가 있는 세부 기록사항들을 표현할 수 있는 XML 기반 PHI 문서의 프라이버시 보안을 보장하기 위한 보안 스펙을 설계한다. 이러한 연구는 구체적인 PHI 문서 스펙이 있어야만 가능하므로 MyPHR[9]이라는 XML 기반 PHI 프로토타입 스펙을 바탕으로 한다. 그리고 보안 스펙은 보안 관련 연구 분야에서 기연구된 접근통제 기법[3]과 XML 암호화[4-6]를 적용한다.

1. MyPHR

PHI를 XML 문서로 표현하면 일반적으로 최상위 요소 하위에 헤더 요소와 컨텐츠 요소를 둔다. 헤더 요소는 문서 관리 정보들을 여러 개의 하위 요소들로 나타내고, 컨텐츠 요소는 PHI 자체 정보를 세분화한 세부 정보들을 표현한 요소 트리로 나타낸다. MyPHR도 최상위 요소(MyPhr) 아래에 헤더(MyPhrHeader)와 컨텐츠(MyPhrBody)를 둔 XML 문서이다.

MyPhrHeader 헤더 요소는 문서 작성자 정보(creatorsInfo), 문서제공 진료기관 정보(clinicsInfo), 문서작성 기간(scopePeriod), 암호키 정보(securityKeyInfo), 문서 생성 정보(documentInfo), 보안 관련 정보(securityLevel, signatureInfo) 등의 문서

관리 정보들을 각각 하위 요소로 두고 있다. 이 중에서 문서 생성 정보와 보안 관련 정보는 보호구역(protectedInfo) 요소로 감싼다.

MyPhrBody 요소는 PHI의 내용을 유형별로 구분하여 분리 기록한 하나이상의 MyPhrModule을 포함한다. MyPhrModule은 preface 요소와 content 요소로 구성되는데, preface 요소에는 해당 모듈에만 적용되는 PHI를 제공한 진료기관(clinicsInfo), 진료정보 기록기간(scopePeriod) 등을 표시한다. content 요소에는 유형별로 구분된 실제 모듈 내용이 기록된다.

각 MyPhrModule 요소는 PHI를 모듈별로 분류한 유형들 중에 한 유형의 기록들을 보관한다. MyPHR은 PHI를 (Table 1)과 같이 9개의 유형으로 분류하고 있다. 이러한 분류는 의료기관에서 사용하는 진료기록 분류를 그대로 따르고 있다. 모듈 유형은 MyPhrModule 요소의 moduleType 속성에 표시된다.

Table 1. MyPhrModule types

유형	설명
person information	개인 신상정보
health insurance information	공공의료보험과 보험사 건강보험 관련 정보
person history information	가족병력, 탄생, 면역이력 생활습관 관련 정보
basic clinic information	알레르기, 혈액형, 감염 관련 이력 정보
illness information	개인 병력
clinical notes information	의료기관 진찰기록
test history information	의료기관 검사기록
surgery record information	의료기관 수술기록
clinical summary information	의료기관 퇴원요약

MyPhrModule의 content 요소는 모듈 유형별로 하나 이상의 섹션으로 구성된다. 섹션은 모듈을 세부적으로 더 분류한 단위인데, person history Information 모듈과 basic clinic information 모듈이 여러 개의 섹션을 가지고 있다. MyPhrModule의 각 섹션에는 해당 유형의 건강기록이 표시되는데, 유형별로 고유의 스펙을 갖는다.

2. PHI 프라이버시 보안

휴대하고 있는 PHI 문서 즉 MyPHR 문서의 프라이버시 보안을 보장하려면, 사용자가 절차에 따라 PHI 문서에 접근하도록 하여야 하고, 절차를 따르지 않는 접근은 PHI 문서의 내용을 볼 수 없도록 해야 한다.

접근 절차는 PHI를 관리하는 시스템에 의해 수행되는데 사용자 식별(Identification), 사용자 인증(Authentication), 허가(Authorization) 순서로 된 일련의 인증허가 과정이다. 식별 과정은 시스템에게 사용자의 식별자(ID)를 요청하는 과정으로 사용자들은 PHI를 관리하는 시스템이 확인할 수 있는 유일한 식별자를 갖는다. 인증은 PHI에 접근할 수 있는 사용자의 능력이나 자격을 검증하는 단계이다. 허가란 사용자, 프로그램 또는 프로세스에게 허가한 권한을 의미한다. 허가를 한다는 것은 사용자가 접근을 해 왔을 때 미리 설정된 권한을 실제로 확인하는 접근통제 과정이다. 접근통제 과정은 어딘가에 보관된 접근통제목록을 사용한다.

지금까지 기술한 PHI 문서의 프라이버시 보안은 PHI 문서에도 보안 스펙을 포함하도록 하고 있다. 즉 접근 통제에 필요한 접근통제목록을 XML 구문 형식으로 포함하고 있어야 하며, 절차를 따르지 않는 접근은 PHI 문서의 내용을 볼 수 없도록 암호화된 내용을 XML 구문 형식으로 표현하여야 한다. 이를 위해 본 연구는 접근통제 기법과 XML 암호화를 사용한다.

III. 결 과

프라이버시 보안을 위해 본 연구에서 PHI 문서에 XML 구문 형식으로 구현한 접근통제목록과 암호화 구조를 기술한다.

1. 접근통제목록

접근통제기법에는 임의적 접근통제, 강제적 접근통제, 비임의적 접근통제가 있으나, 본 연구는 PHI에 접근제어목록(ACL: Access Control List)을 사용하는 임의적 접근통제를 사용한다. 임의적 접근통제기법은 사용자나 소속 그룹의 신원(Identity)에 근거하여 PHI에 대한 접근을 제한하는 방법이다. 임의적 접근통제 정책은 접근통제목록으로 표현된다. 접근통제목록은 PHI에 대한 접근이 허가된 주체들과, 이들 주체가 PHI에 접근할 수 있는 허가받은 접근 종류들이 기록된 목록이다.

MyPHR은 (Table 2)와 같이 5가지 주체를 정의하고, 각 주체별로 none, read, write, delete, all 등 5가지 접근 종류를 지정할 수 있게 하였다. 그리고 접근통제목록은 MyPHR 내에 하나의 요소로 표현하여 허가 정보를 MyPHR에 통합하였다.

Table 2. Access subject types

Type	Description
all	All accessing persons
creator	Creator(writer) himself/herself
owner	Person who is being written about
doctor	Clinical doctor
agent	First-aid agent

(Fig 1)은 owner에게 all 권한을 부여하고 doctor에게 read 권한을 부여한 접근통제목록 요소

(securityLevel)의 예이다.

```
<securityLevel>
  <accessRight permit="all">owner</accessRight>
  <accessRight permit="read">doctor</accessRight>
</securityLevel>
```

Figure 1. Access control element

MyPHR의 접근통제목록은 MyPhrHeader 요소와 MyPhrModule 요소에 둘 수 있다. 이들 접근통제목록은 각각 MyPhrBody, MyPhrModule의 접근을 통제한다. 즉 MyPhrBody에 접근하려면 MyPhrHeader에 선언된 접근통제목록에 명시된 접근권한에 의해 제한을 받고, MyPhrModule에 있는 content 요소의 접근은 MyPhrModule의 preface 요소에서 선언된 접근통제목록에 선언된 접근권한을 따른다.

2. 암호화 구조

XML 암호화는 암호문, 키 정보, 알고리즘을 포함하거나 참조하는 XML 요소(EncryptedData 혹은 EncryptedKey)로 이루어진다. EncryptedData 요소는 암호문을 포장하거나 참조하는 XML 암호화에 의해 만들어진다. 본 연구에서는 PHI가 표시되는 MyPhrBody 요소의 내용을 둘러싼 암호화로 형태로 만든다. 둘러싼 암호화는 데이터를 (Fig. 2)와 같이 CipherValue 요소의 내용으로 한다.

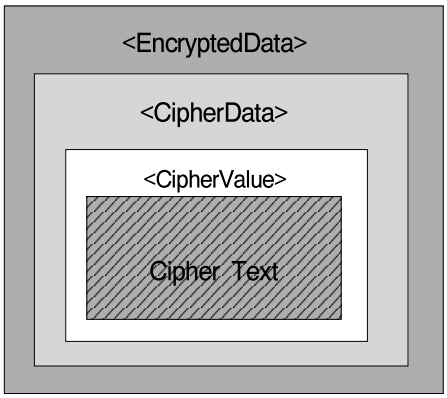

Figure 2. Enveloping XML Encryption

알고리즘과 키 혹은 다른 정보를 포함한 암호화에

```
<EncryptedData Id="EncryptedBody"
  xmlns="http://www.w3.org/2001/04/xmlenc#">
  <EncryptionMethod Algorithm="http://www.w3.org/
    2001/04/xmlenc#aes128-cbc" />
  <ds:KeyInfo
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:RetrievalMethod URI="#EKey" Type=
   "http://www.w3.org/2001/04/xmlenc#EnctryptedKey" />
    <ds:KeyName>MasterEKey</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue>...</CipherValue>
  </CipherData>
</EncryptedData>
```

Figure 3. EncryptedData element

대한 모든 정보를 암호화한다면, 이것은 쓸모없는 정보가 될 것이다. 왜냐하면 복호화에 필요한 정보를 얻기 위해서 복호화를 해야 하기 때문이다. 그래서 EncryptedData 요소는 내부에 (Fig 3)과 같이 EncryptionMethod 요소와 KeyInfo 요소에 각각 알고리즘과 키를 보관한다.

MyPhrBody 요소의 내용을 암호화하기 위해 대칭키를 사용하는데, 이 키는 지정된 사용자의 공개키로 암호화하여 KeyInfo 요소에 둔다. 하지만 본 연구에서는 암호화에 사용한 키를 다른 보안구조(예, 전자서명)에서도 사용할 수 있도록 KeyInfo 요소에는 키를 두지 않고, (Fig 4)와 같이 EncryptedKey 요소로 만들어 MyPhrHeader의 securityKeyInfo 요소에 별도로 보관한다.

```
<EncryptedKey Id="EKey" xmlns=
  "http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
  <ds:KeyInfo
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>Lee Han Su</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue>j230fw</CipherValue>
  </CipherData>
  <CarriedKeyName>MasterEKey</CarriedKeyName>
</EncryptedKey>
```

Figure 4. EncryptedKey element

securityKeyInfo는 내부에 securityKey 요소를 하나이상을 두어 지정된 사용자가 여러 명인 경우 각각 해당 공개키로 암호화하여 보관한다. 가령 MyPHR 문서가 특정 개인을 위해 발행되었더라도 응급처치에서 구급대원이 직접 문서에 있는 PHI를 살펴볼 수 있게 하려면 문서 소유자 외에도 구급대원의 공개키로 암호화한 키를 함께 문서에 보관할 수 있어야 한다.

3. 결과 분석

특정인의 PHI를 MyPHR로 작성한 후 본 연구에서 구현한 프라이버시 보안 스펙을 적용하면 (Fig 5)와 같다. 전체적으로는 XML 형식으로 되어 있으면서 중요 문서 관리 정보(protectedInfo)와 PHI 내용(MyPhrBody)은 암호화되어 있어서 접근이 불가능하다. 접근을 하려면 전용 관리 시스템에 의해 securityKeyInfo 요소에 암호화되어 담겨 있는 암호키를 얻어 protectedInfo 요소와 MyPhrBody 요소를 복호화하여야 한다. 복호화된 문서는 전적으로 관리 시스템에 의해 관리되므로 시스템 외부에서는 파악할 수 없다. 또한 관리 시스템에 의해 복호화된 문서는 자체에 표현된 접근통제목록에 의해 접근이 허가된다. 접근 통제 목록은 암호화되어 나타나지 않으나 문서를 복호화하면 protectedInfo 요소와 MyPhrBody 요소 내에 포함되어 있다. 이상의 분석으로 본 연구에서 구현한 보안 스펙이 XML 기반

PHI 문서의 프라이버시 보안에 필요한 조건을 만족함을 검증하였다.

```
<MyPhr version="1.0" createDate="2006-06-30T11:12:01"
 xmlns="http://www.kmu.ac.kr/MyPHR">
 <MyPhrHeader>
  <creatorsInfo>
   <creator>
    <personalId type="national">670217-1691127</personalId>
    <personalName>김철수</personalName>
    <department>건강증진센터</department>
    <facility>한국의료원</facility>
   </creator>
  </creatorsInfo>
  <clinicsInfo>
   <clinicalFacility>한국의료원</clinicalFacility>
  </clinicsInfo>
  <scopePeriod start="2004-01-01" end="2006-06-20"/>
  <securityKeyInfo>
   <securityKey class="owner">
    <EncryptedKey Id="EKey"
     xmlns="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
     <ds:KeyInfo
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:KeyName>Lee Han Su</ds:KeyName>
     </ds:KeyInfo>
     <CipherData>
      <CipherValue>j230fw</CipherValue>
     </CipherData>
     <CarriedKeyName>MasterEncryptKey</CarriedKeyName>
    </EncryptedKey>
   </securityKey>
  </securityKeyInfo>
  <protectedInfo encode="true">
   <EncryptedData Id="EncryptedInfo"
    xmlns="http://www.w3.org/2001/04/xmlenc#">
    <EncryptionMethod Algorithm=
      "http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:RetrievalMethod URI="#EKey" Type=
       "http://www.w3.org/2001/04/xmlenc#EnctryptedKey" />
     <ds:KeyName>MasterEncryptKey</ds:KeyName>
    </ds:KeyInfo>
    <CipherData><CipherValue>...</CipherValue></CipherData>
   </EncryptedData>
  </protectedInfo>
 </MyPhrHeader>
 <MyPhrBody encode="true">
  <EncryptedData Id="EncryptedBody"
   xmlns="http://www.w3.org/2001/04/xmlenc#">
   <EncryptionMethod Algorithm=
     "http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
   <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     <ds:RetrievalMethod URI="#EKey" Type=
       "http://www.w3.org/2001/04/xmlenc#EnctryptedKey" />
     <ds:KeyName>MasterEncryptKey</ds:KeyName>
   </ds:KeyInfo>
   <CipherData><CipherValue>...</CipherValue></CipherData>
  </EncryptedData>
 </MyPhrBody>
</MyPhr>
```

Figure 5. Case example of MyPHR document

IV. 결 론

PHI 문서가 서버 저장소를 떠나 PC, 모바일 단말기, 스마트 카드 등의 장치에 보관되어 언제든지 사용할 수 있도록 하는 휴대성을 지원하려면 프라이버시 보안을 보장하여야 한다. 본 연구는 PHI 문서가 접근통제와 암호화 기법으로 프라이버시 보안을 보장하는 방법을 제안하고 PHI 문서에 구현하여야 할 보안 스펙을 설계하였다. 결과 분석에 의하면 프라이버시 보안은 우선 문서 암호화로 보장되며, 암호문 문서를 평문 문서로 변환된 이후에는 문서에 있는 접근통제 목록을 사용한 접근통제에 의해 허가받은 사용자만 사용하도록 하여 보장된다.

참고문헌

1. Kwak YS. International standards for building Electronic Health Record (EHR). Proceedings of 7th International Workshop of Enterprise networking and Computing in Healthcare Industry; 2005 June 18 - 23.

2. Abidi SSR, Han CY, Abidi SR. An intelligent info-structure for composing and pushing personalised healthcare information over the Internet. Proceeding of 14th IEEE Symposium of Computer-Based Medical Systems; 2001 July 225 - 230.

4. Kim GP, Park DS, Lee SJ. Information Security. Seoul(KOR):Jungil Press; 2002.

5. O'Neill M, Hallam-Baker P, Cann SM, Shema M, Simon E. Watters PA, et al. Web Services Security. Berkeley(CA):McGraw-Hill/Osborne; 2003.

6. Eastlake DE III, Niles K. Secure XML: The New Syntax for Signatures and Encryption. 1st ed. Boston(MA):Addison-Wesley Professional; 2003.

7. Dournaee B. XML Security. New York(NY):McGraw-Hill; 2002.

8. Bang DW. MyPHR Specification Version 1.01. Available at: http://cee.kmu.ac.kr. Accessed August 29, 2006.