Journal of Korea Multimedia Society Vol. 8, No. 11, November 2005(pp. 1520-1530)

계층적 키 할당 기법을 기반으로 하는 XML 문서의 접근제어

반용호[†], 김종훈[††]

요 약

XML이 인터넷상에서 문서를 표현하고 교환하기 위한 표준으로 인식되면서 XML에 대한 보안 요구가 커지고 있다. 최근까지 XML 보안에 관한 연구는 암호화나 전자서명 같은 기밀성이나 무결성에 관한 연구에 그 초점이 두어져 왔다. 그러나 XML 데이터가 방대해지고 복잡해짐에 따라 XML 데이터를 이용하는 이용자의 권한에 따라 접근을 허용하거나 거부할 수 있는 관리적인 측면에서의 보안 기법의 연구가 요구된다. 이를 해결하기 위해서는 XML에 대한 접근제어 정책을 규정하고 수행하기 위한 모델과 메커니즘이 필요하다. 본 논문에서는 XML로 구성된 문서를 보안 영역 별로 구분하고, 역할기반 접근제어(RBAC)를 응용하여 각 사용자에 대한 역할을 할당하고, 역할에 따른 영역별 암호화를 통하여 특정 문서에 대한 접근제어를 수행하는 새로운 방식의 접근제어 모델과 메커니즘을 제안한다. 본 논문에서 제안하는 방식은 보안 계층이 추가 되거나 삭제되는 경우 해당 보안 계층 간의 관계만을 갱신함으로서 암호화에 사용된 모든 키를 갱신할 필요가 없다는 장점을 가진다.

Access Control to XML Documents Based on Hierarchical Key Assignment Scheme

YongHo Ban[†], JongHun Kim[††]

ABSTRACT

As XML is recognized as a prevalent standard for document representation and exchange in the Internet, the need for security of XML becomes very important issue. Until now researches on XML security have been focused on confidentiality or integrity like encryption and digital signature technology. But, as XML data becomes more massive and complicated, it requires managerial security that decided access permit or deny by the authority of user who is using the XML data. Thus it requires models and mechanisms enabling the specification and enforcement of access control policies for XML documents. In this paper, we suggest the new access control model and mechanism that separate XML documents by access level, assign roles to each user by applying Role Based Access Control (RBAC) and perform access control to specific documents by encrypting each section with roles. The method, we suggested, has an advantage that it does not need to update the whole keys used in encryption process by updating only the relations between appropriate secure layers.

Key words: XML Security(XML 보안), Access Control(접근제어), RBAC(역할기반 접근제어), Hierarchical Key Assignment(계층적 키 할당)

※ 교신저자(Corresponding Author) : 반용호, 주소 : 부산광역시 사하구 하단2동 840번지(604-714), 전화 : 051)200-5590, FAX : 051)200-7783, E-mail : gaussian@donga.ac.kr
접수일 : 2005년 6월 13일, 완료일 : 2005년 10월 4일
[†] 준회원, 동아대학교 컴퓨터공학과 박사수료

[††] 종신회원, 동아대학교 컴퓨터공학과 교수
(E-mail : jhkim@dau.ac.kr)
※ 본 논문은 2002학년도 정보통신부 IT관련학과 장비지원 사업의 동아대학교 대응자금에 의하여 연구되었음.

1. 서 론

XML은 플랫폼과 응용 프로그램에 독립적으로 사용될 수 있고, 태그의 확장이 가능하다는 장점 때문에 인터넷을 기반으로 하는 웹 환경에서 다양하게 활용되고 있다.[15] XML을 사용하고 있는 환경, 즉 웹 환경은 언제나 사용자들이 쉽게 접속하여 필요한 데이터를 주고받을 수 있는 개방형 환경을 특징으로 가지고 있다. 개방형 환경은 사용자들이 쉽게 지정된 데이터에 접속할 수 있는 장점을 제공하지만, 다양한 보안상 문제점들도 계속해서 언급되고 있다. 이를 해결하기 위해서 XML에 관련된 다양한 보안 기법들에 대한 연구가 진행되고 있는데, 이중 대표적인 것은 W3C에서 표준화가 이루어진 XML 전자서명(Signature), XML 암호화(Encryption) 등을 예로 들 수 있다.[16-18] 그러나, XML 문서의 암호화는 단순한 통신상의 보안만을 제공할 뿐 관리적 요소인 다양한 사용자와 다양한 접근권한 정책을 반영하지 못하고 있다. 예를 들어, 의료 환경에서의 환자 정보는 각기 다른 수준의 접근제어를 통해 각 환자의 병명, 병력과 같은 기록들은 제한된 사용자 그룹 중 극히 일부에게만 제공되어야 하는 아주 민감한 정보와 함께 환자의 이름, 전화번호, 주소와 같은 보다 덜 민감한 정보를 포함하고 있을 수 있다. 이런 각각의 항목들은 각기 다른 수준의 접근제어를 반드시 필요로 한다. 접근제어 구현의 핵심적인 요구사항은 XML 문서의 특성에 맞도록 접근제어 모델과 메커니즘을 설계하는 것이다. 이러한 모델과 메커니즘은 사용자 그룹 사이에서 민감성이 다른 정보를 포함하고 있는 XML 문서의 선택적인 배포를 할 수 있는 기능이 매우 중요하다.

본 논문에서는 XML로 구성된 문서를 보안 영역별로 구분하고, 역할기반 접근제어(Role Based Access Control, 이하 RBAC)를 응용하여 각 사용자에 대한 역할을 할당하고, 역할에 따른 영역별 암호화를 통하여 특정 문서에 대한 접근제어를 수행하는 새로운 방식의 접근제어 모델과 메커니즘을 제안한다. 본 논문에서 제안된 방식은 보안 계층이 추가 되거나 삭제되는 경우에 해당 보안 계층 간의 관계만을 갱신함으로서 전체 암호화에 사용된 전체키를 갱신할 필요가 없기 때문에 키 관리의 효율성을 제공한다. 즉, 본 논문에서는 기존에 제안된 XML 문서에 대한 접근제어 방식의 한계를 극복하기 위하여 RBAC를 채택하고, XML 문서가 가지는 계층적 구조를 각각의 영역으로 구성하는 계층 구조로 사용될 수 있도록 하였다. 본 논문의 나머지 부분은 다음과 같이 구성된다. 본 논문의 2절에서 RBAC 특징과 계층적 키 관리에 대하여 설명한다. 3절에서는 RBAC와 계층적 키 할당 방법을 기반으로 하는 새로운 방식의 XML 문서에 대한 접근제어 모델을 제안하고, 제안된 모델이 가지고 있는 주요 특징들을 기술한다. 4절에서는 제안된 모델을 기반으로 XML 문서를 권한에 따라 관리하는 접근제어 메커니즘 중 핵심 요소인 키 유도와 생성, 역할 관리에 대하여 설명한다. 5절에서는 본 논문에서 제안된 모델의 보안성 및 이전 연구들과 본 논문에서 제안된 방식을 비교하여 제안된 방식이 가지는 특징과 차이점을 기술하고, 6절에서는 결론 및 추가적으로 진행되어야 할 연구 방향을 제시한다.

2. 관련 연구

본 절에서는 접근제어를 위한 기존의 모델과 구성요소에 대한 이전의 연구들을 살펴본다. 먼저, Rivi.S 등이 제안한 RBAC에 대한 특징을 설명한다. 2.2절에서 계층적 키 관리에 대하여 설명한다. 마지막으로 기존에 제안된 XML을 위한 접근제어 모델의 특징과 한계점을 언급한다.

2.1 역할기반 접근제어

RBAC는 역할에 근거하여 많은 형태의 접근제어 정책들을 표현하기 위한 접근방법이다. RBAC의 중심적인 개념은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 하는 대신에, 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이러한 개념은 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점을 가진다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없이도 역할의 변경을 쉽게 할 수 있다. 그림 1에서 RBAC의 기본 모델을 보여준다. 기본 모델은 사용자(U), 역할(R), 인가권한(P), 세션(S)으로 구성된다.[1,2]

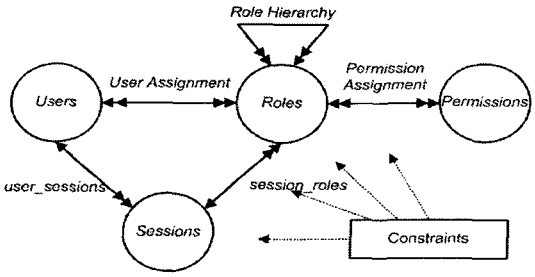


그림 1. 역할기반 접근제어 모델

2.2 키를 이용한 계층적 접근제어

계층에서의 키 관리 문제를 위하여 Alk와 Taylor (이하, AT)는 보안 레벨의 계층에 대하여 대칭암호화 방식의 키 할당 기법을 제안했다.[3] 이 기법의 특징은 만약 사용자 u가 보안 계층 m에 할당되었다면, 사용자 u는 보안계층 $m' \le m$이 되는 모든 계층을 복호화 할 수 있다. AT 방식은 다음과 같이 요약된다. 먼저, 각 보안계층 SC_i는 공개된 정수 t_i를 선택한다. SC_i의 비밀키 SK_i는 $SK_1 = SK_0^{t_i} \pmod m$에 따라 계산된다. 여기서, SK_0는 CA의 비밀키이고, m은 두 소수 p, q의 곱이다. 만약, $SC_j \le SC_i$이 유지된다면, t_j/t_i는 정수이고, 추론에 의하여 SC_i는 SK_j를 유도할 수 있다 : $SK_j = SK_0^{t_j} = SK_0^{t_i * (t_j/t_i)} = SK_i^{(t_j/t_i)} (\mathrm{mod} m)$. 이에 반하여, $SC_j \not\le SC_i$ 인 경우, t_j/t_i의 계산 결과는 정수가 될 수 없으므로 키 유도는 불가능하다. 이후 연구에서 계층적 구조에서의 키 관리 문제는 정규할당 방법을 이용하여 t_i의 값을 줄이는 방법, bottom-up 키 생성 체계를 이용하는 방법들과 함께 동적으로 보안계층을 추가하거나 삭제하는 기법들이 제안되었다.[4, 6-10]

2.3 XML 문서의 접근제어

XML 문서의 접근제어를 위해 이전에도 많은 연구가 수행되었다.[11-14] 그림 2의 문서는 병원에서 사용되는 환자정보를 나타내는 XML 문서를 보여준다. 그림 2에서 보이는 문서에 대한 접근제어를 위한 가장 효율적인 방법은 무엇인가?

이러한 질문에 대한 이전의 연구는 크게 두 가지로 요약된다. 첫 번째 방법은 그림 2와 그림 3의 문서를 문서 전체 또는 각 엘리먼트에 대한 암호화를 수행하여 DB에 저장 후, 각 사용자에게 암호화된 정보를

```
<? XML Version="1.0" encoding="euc-kr"?>
<PatientRecords>
 <Patient Name="Alice">
  <Personal>
   <RRN> 750305-1234567 </RRN>
   <YMD>
     <Year>1975</Year>
     <Month>03</Month>
     <Date>05</Date>
   </YMD>
  </Personal>
  <Medical>
   <Doctor>KimJH</Doctor>
   <Nurse> BaeKM</Nurse>
   <Diagnosis> cold </Diagnosis>
   <Prescription> Chemo medicine </Prescription>
   <Bill> 100,000 </Bill>
  </Medical>
 </Patient>
</PatientRecords>
```

그림 2. 개인 정보를 포함하는 XML 문서의 예

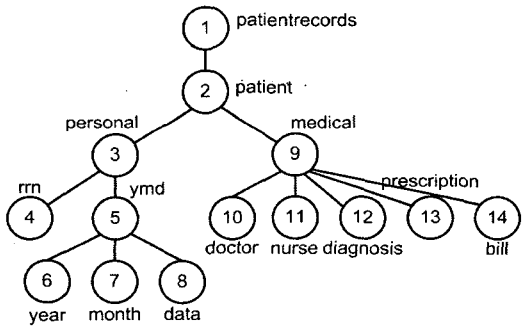


그림 3. 그림 2에 대한 계층적 표현

복호화 할 수 있는 키를 안전한 방법으로 배포하여 각 사용자가 적절한 키를 이용하여 해당 문서를 복호화하여 필요한 정보를 열람하게 하는 기법이 그것이다.[17] 암호화를 수행 하는 기법에 따라 몇 가지 방식이 제안되었는데, Christian 등이 제안한 방법은 기존의 XML 문서의 암호화가 다양한 사용자를 위한 암호화 기법을 제공하지 않는다는 것에 착안하여 XML 문서의 암호화에 접근제어 개념을 도입하여 다른 권한을 가진 다양한 사용자를 위한 암호화 기법을 제안하였다.[11] 하지만 이 방식은 접근을 요청한 사용자에게 권한이 존재 하는 노드들만을 전달하기 위해서 각 노드마다 권한이 존재하는 사용자들의 집합을 유지하고 있어야 한다. 만약 문서의 대부분이 다

른 권한을 가진 다양한 사용자에 대한 기밀 정보라면 문서의 대부분의 노드를 각기 다른 키로 암호화 하는 과정이 요구된다. 이 경우 키의 수가 증가하게 되고, 각 기밀 노드는 키의 분배 문제와 암호화, 복호화를 위한 처리 능력도 높아야 한다. 또한 암호화된 노드들을 분리하여 풀에 저장하므로 각 노드에 원래의 위치를 찾기 위해 트리에서 위치 정보뿐만 아니라 다른 노드의 위치정보를 확인해야만 자신의 위치를 찾을 수 있는 하는 단점을 가진다.

또 다른 방법은 해당 문서를 DOM 트리로 변환하여 각 노드에 대한 접근 권한을 명시하여 사용자가 요청한 권한과 비교 후, 접근이 승인된 노드 집합을 재구성하여 반환함으로서 해당 문서에 대한 적절한 접근제어를 수행하는 방법이다. Securing XML Documents에서 제안하는 접근제어 모델은 DOM 트리를 이용하여 XML 문서와 DTD의 엘리먼트에 접근권한을 설정하고, 설정된 접근권한 정보에 의해 사용자의 XML 문서의 접근을 제어한다.[12] Bertino 등의 XML 파일에 대한 접근제어 모델[13]과 구현 시스템 Author -X [14]의 기본적인 접근제어 방법은 [12]와 같으며, DTD와 XML 파일에 적용되는 여러 형태의 동작(navigation, browsing 등)에 대한 접근제어에 대한 접근제어가 추가 되었다. 그러나 위의 방법들은 사용자의 요구에 대해 DOM 트리를 생성하므로 다수의 사용자가 동시에 동일한 데이터에 접근할 때 사용자가 요구하는 데이터에 대해 매번 DOM 트리를 생성해야 하는 단점이 존재한다.

3. 계층적 키 할당 기법을 이용한 XML 문서의 접근제어 모델

본 절에서는 계층적 키 할당 기법을 이용한 XML 문서의 접근제어 모델을 제안한다. 계층적 키 할당 기법을 이용한 XML 접근제어 모델은 객체에 대한 접근제어 수준을 정의하는 보안등급과 사용자들에게 할당되는 접근권한을 정의하는 보안계층, 권한부여 과정을 통하여 접근 가능한 객체에 대하여 수행가능 한 동작(action)들의 집합인 연산 등으로 구성되고, 이들 구성요소를 기반으로 접근제어 정책에 따라 접근제어가 수행된다. 먼저 3.1절에서는 본 논문에서 제안한 접근제어 모델의 구성 요소를 설명하고, 3.2절에서 본 모델을 위해 정의된 접근제어 정책에 대하여 설명한다.

3.1 제안된 모델의 구성요소

■ 객체

접근제어 정책에서 접근제어의 대상이 되는 자원들의 집합을 객체라고 정의한다. 본 논문에서는 접근제어 객체를 특정 Schema나 DTD를 따르는 XML 문서의 엘리먼트와 속성을 객체로 정의한다. 엘리먼트와 속성은 XPath나 XPath Filter에 의해 구분된다.

■ 보안등급(Security Clearance)

보안등급은 문서에 대한 접근제어의 수준을 나타낸다. 문서에 대한 보안등급은 문서 정보를 제공한 제공자나, 문서를 최종적으로 관리하는 보안 정책 및 이를 관리하는 관리자에 의해 정의된다. 본 논문에서는 전개의 편의를 위하여 관리자가 문서의 등급을 결정한다고 가정한다. 문서에 대한 보안등급은 다음과 같이 결정된다. 먼저 XML 문서 작성을 위한 Schema 작성 시 사용된 엘리먼트와 속성에 정의된 모든 요소에 대한 보안등급 참조사전(Security Clearance Reference Dictionary)을 작성한다. SCRD를 기반으로 XML 문서의 작성에 사용된 엘리먼트 및 속성에 대한 보안등급 정보를 담은 파일을 작성한다. 만약, Schema를 따르지 않는 문서인 경우 실제 XML 문서의 각 엘리먼트로부터 직접 보안등급 정보를 추출할 수 있다.

■ 보안계층(Security Class)

보안등급이 문서에 대한 접근 가능한 수준을 나타내는 반면에 보안계층은 사용자들에 할당되는 접근권한을 의미한다. 보안등급에 보안 계층이 n대 1로 결합된다. 보안계층은 2절에서 언급된 RBAC의 방식을 준용한다. 즉 각각의 사용자는 각 역할 계층에 할당되고, 역할계층은 보안계층 중 하나를 할당 받는다. 보안 계층들은 순서집합(partially ordered set) $U = \{u_1, u_2, \ldots u_n\}$으로 나타낼 수 있으며 각 계층은 기호 '≤'를 이용해서 서로의 관계를 나타낼 수 있다. 만약 $u_1 \leq u_2$인 경우, u_2는 u_1의 상위계층 또는 같은 계층이며, u_2는 u_1이 가지는 정보에 접근할 수 있지만 반대의 경우는 허용되지 않는다.

■ 연산(Operation)

접근제어 모델에서 연산은 권한부여 과정을 통하여 접근 가능한 객체에 대하여 수행가능 한 동작(Action)들의 집합으로 정의할 수 있다. 즉 수행 가능

한 동작을 A라 하고, 대상 객체 집합을 O, 연산을 P 라고 할 때, $P=(O, A)$로 나타 낼 수 있다. 접근제어 모델에서의 연산 유형은 사용되는 모델의 형태에 따라 다양하게 정의될 수 있다. 그러나 본 논문에서는 읽기 연산에 그 초점을 두고 논의를 진행한다. 따라서 본 논문에서는 연산 $P=(O)$로 고정하여 논의한다.

3.2 보안정책

■ 기본 정책

보안정책 수립은 문서에 대한 보안정책과 사용자에 대한 보안정책을 각각 독립적으로 수립한다. 문서에 대한 보안정책은 접근제어가 요구되는 문서에 대한 보안등급을 지정하는 것으로부터 시작된다. 즉, 대상 문서에 포함된 모든 엘리먼트 및 속성에 대하여 적절한 보안등급을 부여한다. (문서에 대한 보안등급은 정보 소유자의 방침에 따라 매우 주관적으로 결정된다. - 문서의 엘리먼트에 대한 보안등급을 결정하는 이유는 주어진 문서를 등급에 따라 암호화를 수행함으로써 전체를 암호화 할 때 발생하는 시간과 자원의 사용을 최소화 할 수 있기 때문이다.) 표 1은 XML 문서에 대하여 작성된 보안등급 테이블의 예를 보여준다.

이제 주어진 문서에 대하여 접근 가능한 계층을 정의하자. 이 과정은 주어진 문서를 사용할 수 있는 사용자들을 그룹별로 지정하는 과정이다. 그림 4의 문서에서 접근 가능한 계층을 정의하면 다음과 같다. 역할계층1-환자(P): 주어진 문서에서 환자 이름이 동일한 Patient 항목을 볼 수 있는 계층으로 정의 한다. 역할계층 2-의사(D): 주어진 문서에서 Medical 부분만 볼 수 있는 계층으로 정의한다. 역할계층3-간호사(N): 환자의 현재 상태만 볼 수 있는 계층이다. 역할계층4-스텝(S): 환자의 이름과 병원비를 볼 수 있는 계층으로 정의한다. 표 2는 그림 4에 대해 접근 가능한 보안계층의 예를 보여준다.

표. 1 hospital.xml에 대한 보안 등급정보

보안등급	E(element)
A	RRN, Diagnosis, Prescription
B	Doctor, Nurse
C	P_Records, P_Name, Personal, YMD, Year ,Month, Date Bill

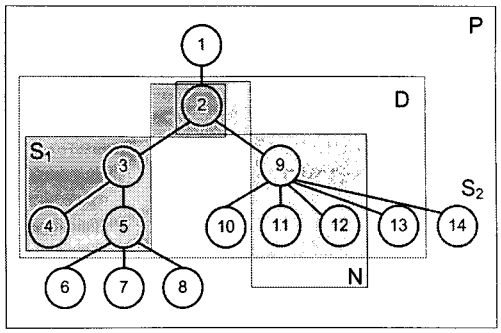


그림 4. 계층별 접근 가능 영역 정의

이제 보안계층 정보를 바탕으로 암호화가 필요한 영역을 각각 정의 할 수 있다. 그림 4는 그림 3에 대하여 표 2의 보안정책을 적용했을 때 얻을 수 있는 암호화 영역을 보여준다. 여기서 객체 P는 환자의 전체 정보, 객체 $D \leq P$는 의사만이 접근 가능한 의료정보, 객체$N \leq P$는 간호사가 접근 가능한 의료정보, $S_1 \leq P$, $S_2 \leq P$는 스텝이 접근 가능한 정보를 의미한다.

■ 역할(정책)계층과 키 계층

<O, ≤>를 객체의 순서집합이라 할 때, 각각의 접근 영역에 대한 깊이 $d(o)$를 계산은 다음과 같이 이루어진다. 먼저 모든 최소 엘리먼트에 대하여, 깊이를 0으로 설정하고, 모든 다른 엘리먼트에 대하여 그것의 가장 높은 자식의 깊이보다 1이 더 큰 깊이로 값을 설정한다. 객체의 집합 O가 주어질 때, 접근제어 정책은 함수 $F : O \rightarrow Z$에 의해 정의된다. $F(o)$는 o의 암호화된 깊이를 나타낸다. 이제 정책 기술 집합 (o, d)와 같이 접근제어 정책을 나타낼 수 있다. $K(o)$는 계층에서 정책 문장(o, d)와 연결된 키를 나타낸다. 계층에서 사용될 마스터키를 정의해야 하는데, 키의 집합 $\{k_1, k_2 \ldots k_n\}$을 가지고 있을 때, $k > k_n$정의함으로서 계층에서의 마스터키를 생성할 수 있다. 마스터 키 K는 계층에서 모든 하위키를 유도하는데 사용된다. 기본적으로 마스터 키는 하나의 역할이기 때

표. 2 hospital.xml에 보안계층 정보

보안계층	접근 가능 항목
환자(P)	문서 전체
의사(D)	환자의 기본 정보/병명/과거 정보
간호사(N)	환자의 기본 정보/병명/처방
스텝(S)	환자의 기본 정보/의료비 내역

문에 퍼미션의 집합에 접근할 수 있다. 그림 5와 그림 6은 그림 4로부터 유도된 역할계층과 키 계층을 보여준다. 그림 6에서 보이는 것처럼 키 K는 $k(N)$, $k(S_1)$, $k(S_2)$, $k(D)$, $k(P)$를 유도하는데 사용 될 수 있다.

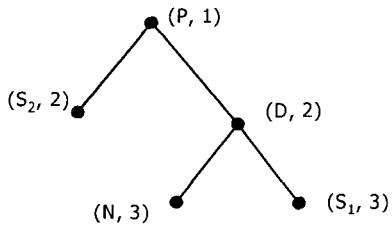


그림 5. 역할계층

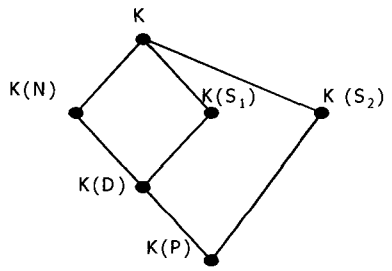


그림 6. 키 계층

3.3 정책의 적용

엘리먼트 영역 N, S_1 그리고 S_2에 대하여 키 $K(N)$, $K(S_1)$, $K(S_2)$를 가지고 각각 암호화를 수행함으로써 정책을 구현할 수가 있다. 다음으로 영역 D(하위 엘리먼트 포함)에 대하여 키 $K(D)$를 사용해 암호화를 수행한다. 마지막으로 영역 P에 대하여 $K(P)$를 사용하여 암호화를 수행한다. 의사 그룹이 해당 영역에 접근하도록 하기 위하여 키 $K(P)$, $K(D)$, $K(N)$, $K(S_2)$가 주어진다. 마찬가지로 환자에게는 전 영역에 접근할 수 있도록 전체 키 $K(P)$, $K(D)$, $K(N)$, $K(S_1)$, $K(S_2)$가 주어진다. 이런 방식으로 각 계층을 각각의 키로 암호화 하고 각 영역을 복호화 할 수 있는 키를 분배한다면 영역별 접근제어는 가능해진다. 그러나 이러한 접근 방법은 다음과 같은 문제를 안고 있다. 각각의 사용자가 어떤 키를 사용하여 복호화를 수행할 것인가? 가장 간단한 방법은 5개의 키 $K(P)$, $K(D)$, $K(N)$, $K(S_1)$, $K(S_2)$를 생성하고, 접근이 가능한 영역에 해당하는 키를 각각의 사용자에게 분배하면 된다. 그러나 XML 문서가 복잡한 형태로 구성된 경우에는 이러한 방법을 적용할 경우 사용자가 매우 많은 키를 관리해야 한다는 어려움이 발생한다. 이러한 문제점을 해결하기 위해서 각 사용자는 하나의 키를 사용하여 문서의 적절한 영역을 복호화 할 수 있도록 하는 접근제어 메커니즘이 필요하다.

4. XML 문서에 대한 접근제어 메커니즘

본 절에서는 3절에서 제안한 모델을 위한 접근제어 메커니즘에 대하여 설명한다. 4.1절에서는 접근제어 메커니즘의 개요에 대하여 설명한다. 4.2절에서는 키 생성과 키 유도에 대하여 설명한다. 본 절에서 사용된 키 생성과 키 유도 기법은 Victor.R.L 등이 제안한 방법을 기반으로 하였다.[5]

4.1 접근제어 메커니즘의 개요

그림 7은 XML 문서의 접근제어를 위한 접근제어 모델의 구조를 보여준다. 제안된 모델은 사용자 인증 모듈과 역할관리 모듈, 보안 계층관리 모듈, 정책관리 서버, CA, XML 쿼리 처리기, XML 문서 저장소 등으로 구성된다. 역할관리 모듈은 각 사용자에 대한 역할의 생성 및 삭제, 새로운 역할의 추가, 각 역할간의 계층관계 등을 정의하고 관리하는 일을 담당한다. 또한 미리 정의된 보안정책에 따라 XML 문서에 대한 암호화를 위하여 역할계층과 키 계층을 서로 연결하고, 이에 관련된 정보를 관리한다. 보안계층 관리 모듈은 XML 문서 저장소에 보관된 전체문서에 대한 보안 등급을 생성 및 삭제, 수정하는 일을 담당한다. 정책관리 서버는 기본 보안정책을 정의하고, 이를 모듈 전체에 적용하는 역할을 담당한다. CA는 문서의 암호화에 사용되는 키를 생성하고 분배하는 역할을 담당한다. 또한 계층 관계 목록을 생성하는 기능을

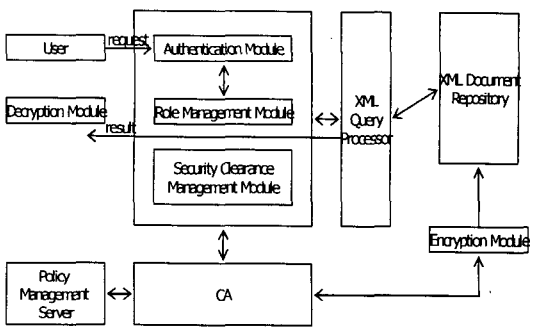


그림 7. XML 문서의 접근제어 모델의 기본 구조

가진다. 계층관계 목록은 계층의 모든 사용자에게 공개된다. 그러나 오직 CA만이 관계 목록의 내용을 수정할 수 있는 권한을 가진다. 암호화 모듈은 주어진 XML 문서에 대하여 접근 가능한 영역에 대한 암호화(XML 문서 저장소 측) 및 복호화(사용자 측)를 수행한다.

4.2 접근제어를 위한 계층적 키 생성과 유도

SK_i를 역할계층 SC_i의 비밀키라 가정하자. 만약 상위 보안계층에 속한 사용자 u_i가 하위계층 u_j의 정보에 접근을 원한다고 할 때, 그는 u_j에 해당하는 비밀 파라미터 b_j를 얻어야 한다. 뉴턴의 다항 보간법(Newton's polynomial interpolations method)에 의하여, 각 사용자는 하위계층의 b를 유도하기 위하여 자신의 키를 사용할 수 있으며, 비밀키는 b로부터 유도될 수 있다. 모든 $SC_j \leq SC_i$에 대하여 CA는 $(j \| (g^{SK_i} \bmod P), b_j)$에서 SC_i에 대하여 $H_i(x)$를 보간한다. 여기서, j는 $1 \leq j \leq P-1$인 SC_j의 식별자, b_j는 비밀 파라미터, $\|$은 결합 연산자를 나타낸다. 그림 5를 바탕으로 CA는 각 점에서의 보간(interpolating)에 의해 계층 P(이하 SC_1)에 대한 $H_1(x)$를 구성한다.

$$(2 \| (g^{SK_1} \bmod P), b_2)$$

$$(3 \| (g^{SK_1} \bmod P), b_3)$$

$$(4 \| (g^{SK_1} \bmod P), b_4)$$

$$(5 \| (g^{SK_1} \bmod P), b_5)$$

CA는 SC_i의 공개 파라미터 Q_i를 계산하여 공개한다.

$$Q_i = (SK_i^{(1/b_i)}) \bmod P$$

$$b_i * b_i^{-1} = 1 (\bmod P-1)$$

비밀 파라미터 b_i가 유도되면, 비밀키 SK_i는 다음 식에 의해 유도할 수 있다.

$$SK_i = Q_i^{b_i} \bmod P = (SK_i^{(1/b_i)})^{b_i} \bmod P = SK_i \bmod P$$

이 과정을 정리하면 다음과 같다.

■ 키 생성 단계

1. CA는 $P = 2P' + 1$이 되는 큰 소수를 선택한다.
2. CA는 $\gcd(SK_i, P-1)$을 만족하는 비밀키 SK_i를 할당하고, $1 \leq b_i \leq P$를 만족하는 양의 정수 b_i를 임의로 선택한다.
3. CA는 모든 $SC_j \leq SC_i$에 대하여 $(j \| (g^{SK_i} \bmod P), b_j)$에서 $H_i(x)$를 보간한다.
4. CA는 공개 파라미터 Q_i를 계산하여 공개한다.

$$Q_i = (SK_i^{(1/b_i)}) \bmod P$$

$$b_i * b_i^{-1} = 1 (\bmod P-1)$$

최종적으로 (b_i, SK_i)를 보안계층 SC_i에 속하는 사용자에게 안전한 채널을 통하여 분배한다.

■ 키 유도 단계

비밀키 SK_i에 의하여, SC_i는 하위계층의 비밀 파라미터 b_j를 유도할 수 있다. 그리고 b_j에 의하여, SC_i는 하위계층의 비밀키 SK_j를 다음 과정에 의하여 유도할 수 있다.

1. $b_j = H_i(j \| (g^{SK_i} \bmod P))$를 계산한다.
2. $SK_j = Q_j^{b_j} \bmod P$를 계산한다.

4.3 역할계층의 관리

본 절에서는 제안된 모델에서 역할계층에 대한 관리 기법에 대하여 설명한다.

■ 역할계층의 추가

기존의 역할계층 구조에서, 새로운 역할계층 SC_k가 SC_i의 하위계층으로 추가 된다. SC_k는 자신의 비밀키를 선택한다. CA는 새로운 계층에 대하여 접근권한을 가진 역할계층의 다항 H_i를 갱신한다. 시스템의 모든 다른 키는 SC_k의 키와 독립적이므로 변경될 필요가 없다. 이를 정리하면 다음과 같다.

1. SC_k의 모든 상위계층인 SC_i에 대하여, CA가 새로운 역할계층 SC_k를 추가한 후에, $(j \| (g^{SK_i} \bmod P), b_j)$에서 $H_i(x)$를 보간한다.
2. SC_k의 모든 하위SC_j에 대하여, $(j \| (g^{SK_i} \bmod P), b_j)$에서 $H_i(x)$를 보간한다.
3. SC_k의 비밀 데이터와 공개 파라미터를 저장한다.

■ 역할계층의 삭제

역할계층 SC_i는 삭제 될 계층 SC_l에 대한 접근권한을 가지고 있다. SC_l이 삭제되기 전에, $H_i(x)$는 계수

k를 가진다고 가정하자. 점 $(l \| (g^{SK_i} \bmod P), b_l)$을 제외하고, CA는 계수 $k-1$을 가지는 새로운 $H_i(x)$를 재구성한다. 여기서, k는 원본 $H_i(x)$로부터 추출된 점들의 개수이다. 즉, CA는 다음 과정을 수행한다.

1. SC_l의 모든 상위 SC_i에 대하여, CA가 SC_l을 삭제한 후에, 점 $(l \| (g^{SK_i} \bmod P), b_l)$을 제외한 점 $(j \| (g^{SK_i} \bmod P), b_j)$에서 $H_i(x)$를 보간한다. 여기서 $SC_j \leq SC_i$, $SC_l \leq SC_i$를 만족해야 한다.
2. SC_l의 비밀 데이터와 공개 파라미터를 삭제한다.

5. 보안성 분석 및 제안된 방식의 고찰

본 절에서는 본 논문에서 제안된 모델에서 사용된 키 생성 기법에 대한 보안성 및 효율성 분석, 그리고 제안된 모델의 기능적 특징들을 이전 연구와 비교하여 본 논문에서 제안된 모델의 특성을 고찰한다.

5.1 보안성 분석

제안된 모델에서 사용된 키 유도 기법에 대한 보안성 분석을 위하여 시스템 내부 또는 외부로부터의 가능한 공격에 대하여 고찰한다.

■ contrary attack

키 유도 단계에서, 보안계층 SC_i는 다항식 $H_i(x)$에 의하여 쉽게 하위계층의 b_j를 유도할 수 있다; 그러나 공격자에게는 이러한 과정이 허용되지 않는다. b_j는 다음 식에 의하여 얻을 수 있다.

$$b_j = H_i(j \| (g^{SK_i} \bmod P))$$

$GF(P)$상에서의 원시근 g를 선택함으로서, b_j는 $GF(P)$상에서 이산대수 계산의 어려움을 기반으로 하는 식으로부터 얻어진다. 이것은 계산 이론에서 가장 어려운 문제 중 하나로 간주된다. 이런 경우에 대하여 이용 가능한 효율적인 알고리즘은 아직 존재하지 않는다.

■ collaborative attack

상위계층에서의 비밀키를 유도하기 위해 하위계층에 속한 사용자의 협업공격에 대한 문제는 contraty attack에서의 단일 사용자 공격과 유사하다. 특정 보안계층에 속한 하위계층의 사용자들은 상위계층의 비밀키를 얻기 위한 협업 공격을 성공 할 수 없다. 예를 들어, SC_i의 자손을SC_x, SC_y, SC_z라 하자. 이 경우 다음과 같은 식을 얻을 수 있다.

$$b_x = H_i(x \| (g^{SK_i} \bmod P))$$

$$b_y = H_i(y \| (g^{SK_i} \bmod P))$$

$$b_z = H_i(z \| (g^{SK_i} \bmod P))$$

주어진 식에 의하여, SC_i의 해를 구하는 것은 $GF(P)$상에서의 이산 대수 계산의 계산의 어려움을 기반으로 한다. 즉, 비밀 파라미터 b가 공개되는 경우에만 상위계층의 비밀키가 노출된다. 즉, 하위계층의 사용자가 상위계층의 비밀 키를 얻기 위한 어떠한 방법도 존재하지 않음을 알 수 있다.

■ interior collecting attacks

S_i, S_{i+1}, S_{i+n}으로 구성된, n개의 부모 노드를 가지는 계층 S_j에 속한 하위권한을 가진 사용자가 존재하는 시스템을 생각해보자. 공격자는 $b_j (j = 0, 1 \ldots n)$의 수집을 통하여 특정 상위계층의 비밀키를 유도하기 위한 시도를 할 수 있다. 이 경우 공격자는 다음 식을 해결해야 한다.

$$b_j = H_i(j \| (g^{SK_i} \bmod P)), \ (i = j = 0, 1 \ldots n)$$

여기서 SK_i의 해를 구하는 것은 $GF(P)$상의 이산대수계산의 어려움을 기반으로 한다.

■ exterior collecting attack

공격자가 시스템의 외부로부터 공격을 시도한다고 가정하자. 공격자는 오직 b_j와 연관된 것을 수집함으로써 하위계층의 비밀키 유도를 위한 시도를 할 수 있다. 이 경우 공격자는 식 $b_j = H_i(j \| (g^{SK_i} \bmod P))$로부터 SK_i를 구해야 한다.$(i = j = 0, 1 \ldots n)$. 그러나 $n+2$개의 미지수에 대한 해를 $n+1$개의 식을 이용하여 얻을 수 없다.

5.2 제안된 방식의 고찰

본 절에서는 본 논문에서 제안된 모델이 가지는 주요 특징을 기존 모델과 비교하여 본 논문에서 제안한 모델의 특징과 필요성에 대하여 고찰한다. 비교의 기준은 일반적으로 요구되는 XML 문서의 보안 요구사항의 만족 여부와 접근제어의 단위, 접근제어 영역

표 3. 제안된 모델의 기능적 특성 비교

비교 항목	RBAC [1][1)]	E. Damiani [12]	Bertino [13]	W3C [17]	Cristian [11]	제안된 모델
기반 모델	RBAC	DAC	DAC	없음	없음	RBAC
메커니즘 구현 방식	-	노드의 필터링	노드의 필터링	암호화	암호화	이산대수를 이용한 암호화
접근제어 수행주체	역할	개별 사용자	개인	개인	개인	역할
접근제어 대상객체	개별 문서	인스턴스 문서	인스턴스 문서	인스턴스 문서 엘리먼트	엘리먼트	인스턴스 문서 엘리먼트
접근제어 영역분할 방식	-	레이블링	레이블링	엘리먼트 지정에 의해	엘리먼트 지정에 의해	객체의 보안등급에 따라
문서에 대한 레이블링 과정	불필요	필요	필요	불필요	필요	불필요
엘리먼트 표현	-	XPath 사용	Xpath 사용	엘리먼트 이름	엘리먼트 이름	XPath 사용
전체 키의 수	-	지원되지 않음	지원되지 않음	노드의 수와 동일	노드의 수와 동일	역할 수와 동일
다중사용자의 동적관리	가능	불가능	불가능	불가능	불가능	가능
객체가 관리하는 키 수	-	지원되지 않음	지원되지 않음	접근하고자 하는 노드 수와 동일	접근하고자 하는 노드 수와 동일	최대 1개
동적 키 관리 지원여부	불가능	불가능	불가능	불가능	불가능	가능

의 분할 방법, 접근제어 수행의 주체, 다중 사용자의 동적 관리, 사용되는 키의 수 등이다.

■ 미세단위 접근제어

XML 문서에 대한 보안 요구사항은 XML 문서는 보안 민감성의 수준이 다른 각각의 요소를 포함할 수 있으므로 이를 만족하는 다양한 보안 계층이 지원되어야 한다. 이러한 요구사항을 만족시키기 위해서는 XML 문서를 위한 접근제어 메커니즘은 최소한의 단위로 보안 정책을 적용할 수 있는 충분한 유연성을 가져야 한다. 본 논문에서 제안된 모델에서 미세 단위 접근제어를 지원은 대상 문서에 대한 접근 가능 영역을 엘리먼트 단위로 정의함으로써 미세단위 접근제어를 지원한다.

■ 접근제어 영역의 분할 방법

기존의 연구에서는 접근제어 영역을 정의하기 위하여 주어진 문서를 트리화하고, 트리화된 문서의 각 노드에 접근제어 정책을 기술하는 방법을 수행하여 접근제어 영역을 분할하였다. 그러나 본 논문에서 제안하는 방식은 주어진 문서에 대한 레이블링 대신 각 엘리먼트에 대한 보안 등급을 정의하고 보안등급에 따라 접근제어 영역을 정의하도록 하였다. 이러한 기법은 주어진 문서에서 접근 제어가 반드시 필요한 영역은 한정되어 있으므로, 접근 제어가 필요한 노드들에 대해서만 보안 등급을 지정함으로써 필요한 보안정책의 수를 줄일 수 있다.

■ 접근제어 주체

기존에 진행된 연구들은 사용자와 접근제어 대상 객체의 관계를 1대1로 지정하는 형태로 접근제어 규칙을 정의하고 적용함으로써 사용자와 접근제어 대상객체 사이에서 1대1의 접근제어는 가능하지만, 대규모의 사용자 또는 대규모의 스키마 문서와 이를 따르는 인스턴스 문서를 가지는 환경에서는 적용이 불가능하다는 한계를 가진다. 그러나 본 논문에서 제안된 모델과 메커니즘은 접근제어 수행 주체를 사전에 부여된 역할 그룹으로 정의하고, 역할 계층에 대하여 명시적으로 접근 가능한 접근제어 목록을 정의함으로서 대규모의 사용자 또는 대규모의 스키마 문서와 이를 따르는 인스턴스 문서를 가지는 환경에서 적용이 가능하다.

■ 다중 사용자의 동적 관리

다중사용자 환경에서의 접근제어 문제에 관한 것으로 동일한 스키마를 기반으로 생성된 인스턴스 문서에 대한 사용자별 접근제어가 반드시 필요하다.

1) 비교대상 [1]은 접근제어 대상을 XML로 하고 있지는 않으나 본 논문의 기반모델로 사용하였으므로 비교 대상에 포함하였다.

즉, 동일한 스키마를 따라 생성된 인스턴스 문서의 정보는 동일한 역할을 부여 받은 사용자 별로 또 다른 접근제어를 수행 할 수 있는 메커니즘이 요구된다.(예를 들어, 동일한 부서에 소속된 의사는 동일한 역할을 부여 받게 되지만, 담당하는 환자의 정보는 모두 틀리므로, 각각의 의사 별로 해당 환자의 기록을 볼 수 있도록 해야 한다.) 본 논문에서 제안된 방식은 각 사용자의 역할의 추가/삭제를 위해 동적으로 키를 생성 및 삭제하는 메커니즘을 적용함으로서 다중 사용자의 동적인 관리를 지원한다.

■ 접근제어에 사용된 키의 수

본 논문에서 적용한 계층적 키 관리기법은 자신의 비밀키로부터 자손의 키를 유도하고, 자신의 키를 유도하기 위해 자손들의 협업 공격의 가능성을 피할 수 있는 보안 계층을 허용한다. 이러한 키 계층의 특징은 XML 문서에 대한 접근제어에서 암호화를 위한 키 생성에 그대로 적용할 수 있다. 즉, 키 $SK(R_1)$, $SK(R_2)$, $SK(R_3)$, $SK(R_4)$, $SK(R_5)$는 문서의 암호화에 사용되고, 각 사용자는 해당 XML 문서의 각 영역을 직접 복호화 하거나, 복호화에 필요한 키를 유도할 수 있도록 키 집합 $\{SK(R_1), SK(R_2), SK(R_3), SK(R_4), SK(R_5), K\}$로부터 단 하나의 키를 부여 받을 수 있다. 이러한 방식은 각 역할 계층 당 1개의 키 만을 필요로 한다는 것을 의미한다. 즉 본 논문에서 제안된 방식에서 사용되는 키의 수는 전체 역할수와 동일하다. 표 3에서 본 논문에서 제안된 모델의 기능적 특성을 기존에 제안된 방식과 비교 분석한 결과를 보여준다.

6. 결 론

본 논문에서는 XML로 구성된 문서를 보안영역별로 구분하고, RBAC를 응용하여 각 사용자에 대한 역할을 할당하고, 역할에 따른 영역별 암호화를 통하여 특정 문서에 대한 접근제어를 수행하는 새로운 방식의 접근제어 모델과 메커니즘을 제안하였다. 본 논문에서 제안된 방식은 보안 계층이 추가 되거나 삭제되는 경우에 해당 보안 계층 간의 관계만을 갱신함으로서 전체 암호화에 사용된 전체키를 갱신할 필요가 없다는 장점을 가진다. 향후에 추가적으로 연구되어야 할 부분은 다음과 같이 요약된다. 먼저, 주어진 XML 문서의 접근하고자하는 사용자의 수가 증가하여 계층구조가 최대한 복잡해질 경우를 고려한 역할 계층 관리 기법 및 키에 대한 연구가 필요하다. 또한 주어진 XML 문서에 대하여 각 엘리먼트 별로 보안등급을 부여하고 보안등급에 따른 암호화 수행할 수 있는 보다 세밀한 접근제어 모델에 대한 연구가 필요하다.

참 고 문 헌

[1] R. Sandhu, E,J.Coyne, and H.L.Feinstein, "Role-based Access Control Models," *IEEE Computer*, Vol. 29, No. 2, pp. 33-47, 1996.

[2] D.Ferraiolo, R.Sandhu, S.Gavrila, D.R.Kuhn, and R.Chandramouli, "Proposed NIST Standard for Rolebased Access Control," *ACM Trans. Inf.Syst.Security*, Vol. 4, pp. 224-274, Aug. 2001.

[3] Selim G. Akl and Peter D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems(TOCS)*, Vol. 1, No. 3 pp. 239-248, Aug. 1983.

[4] MacKinnon, S.T., Peter D. Taylor, Meijer, H., and Selim G. Akl, "An optimal algorithm for assigning cryptographic keys to control access in a hierarchy," *IEEE Transactions on Computers,* Vol. 34, No. 9, pp. 797-802, Sept. 1985.

[5] Victor R. L. Shena and Tzer-Shyong Chenb, "A Novel Key Management Scheme Based on Discrete Logarithms and Polynomial Interpolations," *Computers & Security*, Vol. 21, No. 2, pp. 164-171, 31 March 2002.

[6] Tzer-Shyong Chen and Jen-Yan Huang, "A novel key management scheme for dynamic access control in a user hierarchy," *Applied Mathematics and Computation*, Vol. 162, No. 1, pp. 339-351, 4 March 2005.

[7] Chang, C.C, Hwang, R.J., and Wu, T.C., "Cryptographic Key assignment scheme for access control in a hierarchy," *Information*

System, Vol. 17, No. 3, pp. 243-247, 1992.

[8] Chang, C.C and Buehrer, D.J, "Access control in a hierarchy using a one-way trapdoor function," *Computers and Mathematics with Applications*, Vol. 26, No. 5, pp. 71-76, 1993.

[9] Hui-Min Tsai and Chin-Chen Chang, "A Cryptographic implementation for dynamic access control in a user hierarchy," *Computers & Security*, Vo. 14, No. 2, pp. 159-166, 1995.

[10] Cungang Yang and Celia Li, "Access control in a hierarchy using one-way hash functions," *Computers & Security*, Vol. 23, No. 8, pp. 659-664, Dec. 2004.

[11] Christian Geuer Pollmann, "XML Pool Encryption," *In Proc. of the 2002 ACM workshop on XML security(XMLSEC02), Washington. DC, USA*, pp 1-9, 22, Nov. 2002.

[12] E. Damiani, De Capitani di Vimercati, S. Paraboshi, and P. Samarati, "Securing XML Documents," *In Proc. of the 2000 Int'l Conference on Extending Database Technology (EDBT2000), Konstanz, Germany*, pp. 27-31, March 2000.

[13] E. Bertino, S. Castano, E. Ferrari, and M. Mesiti, "Specifying and Enforcing Access Control Polices for XML Document Sources," *World Wide Web Journal*, Vol. 3, No. 3, pp. 139-151, 2000.

[14] E. Bertino, S. Castano, and E. Ferrari, "Securing XML Documents: the Auther-X Project Demonstration," *In Proc. of the SIGMOD 2001 Conference, Santa Babara(CA)*, May 2001.

[15] www.w3c.org, "eXtensible Markup Language (XML) 1.0," *W3C Recommendation*, 04 Feb. 2004.

[16] www.w3c.org, "XML-Signature Syntax and Processing," *W3C Recommendation*, 12 Feb. 2002.

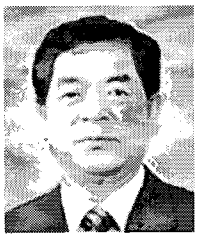
[17] www.w3c.org, "XML Encryption Syntax and Processing," *W3C Recommendation*, 10 Dec. 2002.

[18] OASIS, "eXtensible Access Control Markup Language Version 1.1," 24 July 2003.

반 용 호

1998년 동서대학교 전자공학과 졸업(공학사)
2000년 동아대학교 컴퓨터공학과 졸업(공학석사)
2003년 동아대학교 컴퓨터공학과 박사수료

관심 분야 : 암호이론, 접근제어, 홈 네트워킹 등



김 종 훈

1974년 동아대학교 전자공학과 졸업(공학사)
1977년 동아대학교 전자공학과 졸업(공학석사)
1986년 경북대학교 전자공학과 졸업(공학박사)
1986년~현재 동아대학교 컴퓨터공학과 교수

관심 분야 : 암호이론, 접근제어, HW/SW 통합설계 등