XML문서접근조종을 위한 보안방책작성의 한가지 방법

문명옥, 김광일

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《과학기술을 발전시키는것은 나라의 경제를 빨리 발전시키기 위한 중요한 담보입니다.》(《**김정일**선집》 증보판 제11권 133페지)

XML형태로 작성되는 문서의 량이 급격히 늘어나고있는 오늘 XML문서에 대한 효률적인 관리와 보안을 위한 접근조종이 중요하게 제기되고있다.[1, 3]

XML문서는 특성상 꼬리표들을 리용하여 분할할수 있으므로 XML문서에 대한 접근조종은 전체 XML문서뿐아니라 그것이 포함하는 최상위요소와 하위요소, 속성 등에까지 보안방책을 적용할수 있어야 한다.

그러나 선행한 접근조종방법[2]들은 권한부여의 대상지정에서 유연성이 부족하고 연산에 제한이 있는것으로 하여 유연한 접근조종을 실현하지 못하고있다.

론문에서는 꼬리표에 기초하여 XML문서에 대한 세밀한 접근조종을 진행하기 위한 보안방책의 작성방법을 제안하였다.

1. XML문서에 대한 접근권한

XML문서는 요소(element)들로 이루어져있으며 요소는 하위요소를 포함할수도 있다. 이때 XML문서를 다음과 같은 나무구조로 정의할수 있다.

$$XD = (V_d, v_d, E_d, fE_d)$$

여기서 $V_d = V_{de} \cup V_{da}$, V_{de}는 요소마디들의 모임, V_{da}는 속성마디들의 모임, v_d는 뿌리마디, $E_d = (E_{de} \cup E_{da}) \subseteq V_d \times V_d$는 가지들의 모임으로서 E_{de}는 《요소－하위요소》관계들의 모임이고 E_{da}는 《요소－속성》관계들의 모임이다. 그리고 $fE_d : E_d \rightarrow Label$은 가지에 표식을 붙이는 함수이다.

보안방책을 정의하려면 먼저 주동체와 객체, 접근권한을 정의해야 한다.

론문에서는 사용자에 대한 권한부여에 사용자그룹과 위치패턴을 리용한다. 사용자그룹은 봉사기에 등록된 사용자식별자(ID)들의 모임이며 위치패턴은 수자로 된 IP주소의 어떤 위치의 수자대신 기호《*》를 교체해넣는 방법으로 생성된다.

사용자와 사용자그룹은 성원관계, IP주소는 패턴에 의하여 부분순서화된 모임계층으로 표시할수 있다.

모임 X에 대하여 R가 $X \times X$에서 정의된 부분순서관계일 때 R의 요소들의 모임을 순서쌍 $<X, R>$로 표시한다.

U를 사용자식별자들의 모임, G를 사용자그룹이름들의 모임, $UG = U \cup G$라고 할 때 계층화된 사용자를 다음과 같이 정의한다.

$(x, y) \in UG \times UG$에 대하여 $<UG, \leq_{UG}>$를 사용자라고 부른다. 여기서 $\leq_{UG}$는 성원관계

《x는 y의 성원이다.》이다.

$x \le_{UG} y$ 에 대하여 y는 x보다 상위에 있다고 말한다. UG는 성원관계 $\le_{UG}$ 에 의하여 일정한 계층으로 갈라진다.

I는 수자로 된 IP주소들의 모임, I_P는 IP패턴들의 모임, $A = I \cup I_P$ 라고 할 때 계층화된 사용자의 위치 즉 주소를 다음과 같이 정의한다.

$(x, y) \in A \times A$ 에 대하여 $< IP, \le_{IP} >$ 를 주소라고 부른다. 여기서 $\le_{IP}$ 는 정합관계 《x는 y에 정합된다.》이다.

$x \le_{IP} y$ 는 y의 매 요소가 *이거나 x의 해당 위치의 요소와 같은 경우 성립한다. 이때 주소 y는 x보다 상위에 있다고 말한다. IP는 $\le_{IP}$ 에 의하여 계층화된다.

계층은 x가 y보다 상위에 있을 때 x로부터 y에로 나가는 가지로 련결하는 방식으로 생성되는 방향그라프로 표시할수 있으며 계층에 존재하는 상하위관계는 그라프의 경로에 대응한다.

사용자 $< UG, \le_{UG} >$ 와 주소 $< IP, \le_{IP} >$ 에 기초하여 권한부여를 위한 주동체를 다음과 같이 정의한다.

$AS = UG \times IP$ 이고 $\le_{AS}$ 가 다음과 같이 정의되는 관계일 때 $< AS, \le_{AS} >$ 를 주동체라고 부른다. $(ug_i, ip_i), (ug_j, ip_j) \in AS$ 에 대하여 $ug_i \le_{UG} ug_j$ 이고 $ip_i \le_{IP} ip_j$ 일 때 (ug_i, ip_i) 와 (ug_j, ip_j) 는 관계 $\le_{AS}$ 에 있다고 말한다.

$s_i \le_{AS} s_j$ 일 때 주동체 s_j 는 s_i 보다 상위에 있다고 말한다.

주동체 s_j 에 부여된 권한은 $s_i \le_{AS} s_j$ 인 모든 주동체 s_i 에 적용된다.

XML문서에 대하여 상세한 수준의 보호를 제공하기 위해서는 요소나 요소내의 특정한 속성에 이르기까지의 대상들에 권한을 부여할수 있어야 한다.

론문에서는 XML문서의 임의의 내부구성부분들을 식별하기 위한 경로표현을 다음과 같이 정의한다.

XML문서의 나무구조상에서 기호 /로 구별되는 요소나 속성들의 렬 $l_1 / l_2 / \cdots l_{n-1} / l_n$ 을 경로표현이라고 부른다. 이때 $l_i (l_i \in V_d, \ i = \overline{1, n})$ 는 요소나 속성을 나타내며 $l_1, l_2, \cdots, l_{n-1}$ 을 순차적으로 따라내려가는 방법으로 l_n 에 도달할수 있다.

사용자의 접근요청에 대하여 보호대상으로 되는 XML문서의 구성요소인 객체는 다음과 같이 정의한다.

XML문서에 대한 경로표현을 따라 도달하게 되는 마디 $l_n \in V_d$ 들(요소 또는 속성)을 권한부여객체라고 부른다.

권한부여의 단위인 객체는 XML문서내의 임의의 요소, 속성에 이르기까지 경로표현으로 지정할수 있는 모든 대상을 포괄한다.

5항조 <Subject, Object, Action, Sign, PType>를 XML문서에 대한 접근권한이라고 부른다. 여기서 Action $\in$ {read, write, create, delete}는 주동체가 수행가능한 연산, Sign $\in$ {+, −}는 권한부호로서 《+》는 연산의 허가, 《−》는 거부, Ptype $\in$ {L, R}는 권한의 전파속성으로서 L은 요소에 주어진 권한을 그 요소의 속성들에 전파, R는 요소에 주어진 권한을 그 요소의 모든 하위요소와 속성들에 전파할수 있다는것을 표시한다.

2. 보안방책의 서술과 접근조종

보안방책은 접근권한들의 모임으로서 론문에서는 XML형식으로 서술하여 화일(xml.xas)로 보관한다.

```
<AccessPolicys>
    <policy>
        <subject>
         <user="kgi"/>
        </subject>
        <object href="/paper.xml" path="issues"/>
        <action name="read" sign="+" ptype="L"/>
    </policy>
    … … …
</AccessPolicys>
```

보안방책에 따르는 접근조종알고리듬은 다음과 같다.

입력: rq = (Subject, Object, Action, Sign, Ptype), XML문서, ap: 보안방책 (xml.xas)

출력: 허가된 항목들만으로 된 XML문서

① XML문서에 대한 구문분석을 진행하여 DOM나무 T를 얻는다.

② rq와 ap에 기초하여 T상에서 허가된 요소들에 대한 표식을 붙인다.

③ T에서 표식이 붙은 마디를 제외한 마디들은 제거한다.

④ T에 대응하는 XML문서를 만들어 출력한다.

맺 는 말

XML문서에 대한 접근권한을 꼬리표에 기초하여 정의하고 접근요청시 문서의 특정한 항목들에만 접근하도록 허가하는 방법으로 사용자의 권한에 해당하는 자료만을 제공하도록 하는 XML문서접근방책작성방법을 제안하였다.

참 고 문 헌

[1] 박성호, 박명숙; 콤퓨터망보안, **김일성**종합대학출판사, 21～27, 주체102(2013).

[2] S. Mohr et al.; XML Application Development With XML4.0, Wrox Press, 125～188, 2002.

[3] Raghu Ramakrishnan et al.; Database Management System, McGraw-Hill, 692~723, 2003.

주체108(2019)년 8월 5일 원고접수

A Method to Make Security Schema for Controlling XML Document Access

Mun Myong Ok, Kim Kwang Il

In this paper, we proposed a method to make security schema for controlling detail access to XML document by using tags.

Key words: XML document access, security schema