고도로 분산된 컴퓨팅 환경을 위한 효율적 속성 인증서 관리 기법

양 수 미*

요 약

고도로 분산된 컴퓨팅 환경에서 역할 기반 접근제어를 함에 있어서 속성 인증서를 사용한 역할의 효율적 관리 방법을 모색하고자 한다. 역할은 그룹화되며, 속성인증서를 통해 관리된다. 유비쿼터스 컴퓨팅 환경과 같은 고도의 분산 컴퓨팅 환경에서는 광범위한 통제 구조를 가질 수 없으므로 이를 고려한 속성 인증서 관리 기법으로 속성 인증서의 전송 방법, 그룹 키의 관리 방법 등이 고려되어야한다. 본 논문에서는 네트워크 상의 효율적 속성 인증서 관리 기법을 모색하며, 그의 기반이 되는 역할의 그룹화를 논한다. 역할을 그룹화하여 관계구조 트리를 구성하고, 분산된 환경에서 안전하고 효율적인 역할의 갱신과 분배를 달성한다. 규모 확장성을 위해 멀티캐스팅 패킷을 사용한 속성 인증서 분배를 하며, 그에 따른 네트워크 상의 패킷 손실율을 고려한 성능분석을 하여 역할 그룹을 두어 속성 인증서를 구조화하는 것이 성능을 향상시킴을 정량적으로 보인다.

An Efficient Attribute Certificate Management Technique for Highly Distributed Environment

Soomi Yang*

ABSTRACT

For an efficient role based access control in highly distributed computing environment to reduce management cost, we utilize attribute certificates. Especially highly distributed computing environments such as ubiquitous computing environments which cannot have global or broad control, need another attribute certificate management technique. The techniques for transmission of the attribute certificates and management of the group keys should be considered to reduce management cost. For better performance we structure attribute certificates. We group roles and make the role group relation tree. It results secure and efficient role renewing and distribution. For scalable attribute certificate distribution, multicasting packets are used. We take into account the packet loss and quantifying performance enhancements of structuring attribute certificates.

Key words : Attribute Certificate, Role Based Access Control, Multicasting Communication

* 수원대학교 인터넷정보공학과 교수

1. 서 론

근래의 고도의 네트워크 환경으로 대두되고 있는 유비쿼터스 컴퓨팅 환경은 대량의 네트워크로 연결된 무선 기기가 중앙의 제어없이 자율적으로 상호작용하는 동적 환경으로 대표된다. 중앙의 통제가 없으며 완결되지 않은 채 접속이 종료되는 객체들로 인하여 정리된 전체적 관리 구조가 유지되지도 않는다. 분산된 구조의 분산성을 유지하면서 시스템간의 관계를 정의해야 한다. 반면에 사용자는 어느 시점, 어느 장소에서든지 자원과 서비스에 접속할 수 있기를 기대한다. 이를 지원하기 위해서 자원을 누구에게나 접속가능하도록 하는 경우, 오픈된 네트워크가 가지는 보안상의 문제점을 가지게 된다. 그러한 오픈된 네트워크 환경에서 보안을 고려하기 위해서는 중앙의 통제가 없이 사용자의 인증과 접근제어를 이룰 수 있어야 한다. 현존하는 보안 기반구조가 이러한 증가하는 유연성에 적합하지 않으므로, 이를 위해 인증과 접근제어에 있어서 분산된 신뢰 구조(trust structure)가 제안되었다 [11]. 신뢰 구조에서는 역할 기반 접근 제어를 하며 권한 위임 기법을 쓴다. 본 논문에서는 신뢰구조의 철학을 접근제어를 위한 속성 인증서 관리에 적용, 속성 인증서 간의 신뢰구조를 확립한다. 이것은 신뢰 구조가 가지는 권한 위임과는 다르며, 권한의 분산으로 생각할 수 있다. 역할을 그룹화하여 새로이 역할그룹을 정의하며, 이는 객체를 그룹화하여 역할을 할당하는 기존의 일반적 역할 인증서 사용 방법과는 다른 방식이다.

멀티캐스트는 그룹 통신을 위한 효율적이고 규모 확장성을 가진 기술로 각광받고 있다. 이는 그룹통신을 이용하는 응용을 위해서 뿐만이 아니라 속성인증서의 배분에도 적용되어 효율성을 제공한다. 본 논문에서는 역할 그룹 속성의 분배에 적용되어 효율성과 규모 확장성을 제공한다.

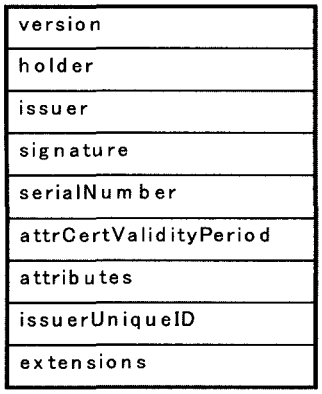
논문의 순서는 다음과 같다. 2장에서 역할 그룹 모델을 설계하고 역할 그룹화를 정의한다. 3장에서 역할 갱신 통신 모델을 정의하고 분석한다. 4장에서 성능 분석 결과를 보이고, 5장에서 요약과 함께 결론을 맺는다.

2. 역할 그룹

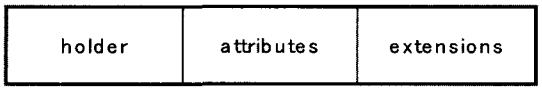
역할 그룹의 구성원들은 그룹 간의 비밀통신을 위하여 대칭적 세션키, TEK(Traffic Encryption Key)를 공유한다. 역할 그룹은 그룹 키를 유지하며 역할로 인한 안전한 그룹 통신을 원할 경우 그룹 키를 사용하게 된다. 역할 그룹은 (G, K, R) 삼원식으로 표현된다. G는 유한하고 비어있지 않은 역할그룹($Group_i$)의 집합이다 $Group_i$는 유한하고 비어있지 않은 역할(r_i)의 집합이다. K는 유한하고 비어있지 않은 키의 집합으로 그룹 키(TEK_i)를 포함한다. R은 G와 K사이의 이원관계로 안전한 그룹 통신에 관여되는 역할 그룹과 그룹 키 사이의 관계를 나타낸다. 그러므로 $R_i \subset G_i \times K_i$가 된다. 그룹 키는 안전한 역할 그룹을 이루는 역할의 집합에 대한 키 서버 KS_i가 키 생성과 분배를 책임진다. KS_i가 생성하는 키는 K에 속한 TEK_i에 해당한다. 키 서버는 역할 그룹과 그룹 키 간의 관계 R_i에 대한 정보를 유지한다. 그룹간의 트리 관계에 따라 그룹 키도 트리를 구성하게 된다.

[4, 5]의 표준에 정의된 속성 인증서의 형식은 (그림 1)과 같다. 각 필드에 대한 설명은 [4, 5]를 참고하기 바란다.

(그림 1)에서 본 논문에서 다루는 필드만으로 간략화된 형식으로 나타내면 (그림 2)와 같다. 이를 이용하여 간략한 표현을 들어 논문의 내용을 설명하고자 한다.



(그림 1)속성 인증서의 형식



(그림 2) 간략화된 속성 인증서의 형식

소유자(holder)에는 공개키 인증서의 주체(subject)에 해당하는 사용자 혹은 역할이름이 올 수 있다. 또한 속성(attributes) 필드에는 역할(role)을 비롯하여 access identity, group, clearance, audit identity, charging identity 등이 올 수 있으며, 경우에 따라 비어있을 수도 있다. 확장(extensions) 필드는 다양하게 정의될 수 있다.

[4, 5]에 정의된 권한 관리 구조(PMI)의 역할 모델에서 속성 인증서는 역할을 holder(주체, 소유자)에게 할당하는 역할 할당 인증서(Role Assignment Certificate)와 정의된 역할에 대한 명세를 가지는 역할 명세 인증서(Role Specification Certificate)로 구분된다. 역할 할당의 변경없이 역할에 대한 명세만을 독립적으로 바꿀 수 있도록 하기 위함이다. 이와 같이 역할의 할당과 명세를 독립적으로 구현하기 위한 속성 인증서의 사용에 있어서 역할 명세 인증서를 쓸 경우, 역할 할당 인증서는 역할 확장 필드에 역할명 또는 역할 명세 인증서 identifier를 가진다. 역할 명세 인증서의 소유자(holder)는 역할 할당 인증서의 역할명(roleName)에 해당한다. 본 논문에서는 속성 인증서가 모든 정보를 가지고 있는 것으로 간주한다.

역할 그룹을 구조화하기 위해 역할을 그룹화한다. 이와 같이 역할을 그룹화하는 것은 기존의 속성인증서의 적용에 있어서 (사용자)그룹에 대해 역할을 주는 것과 다르며, 우선순위를 나타내는 역할의 구성과도 다르다. 역할을 모아 신뢰구조를 수립하는 것이다.

역할 그룹을 두는 경우 권한을 사용하고자 할 때 속성 인증서의 체인을 따라가야하는 경우 성능저하가 있을 수 있다. 그러므로 속성 인증서를 캐쉬하여 효율적 사용이 가능하도록 한다. 캐싱의 방법은 [6]에 제시되어 있고, 본 논문에서는 역할 할당에 변화가 있어 속성 인증서를 갱신해야할 경우에 대해서 논한다.

역할 그룹 인증서로 속성 인증서 혹은 공개키 인증서를 이용할 수 있다. 공개키 인증서를 사용할 경우, 확장(extensions) 필드에 역할 그룹에 관한 정보를 가지게 된다.

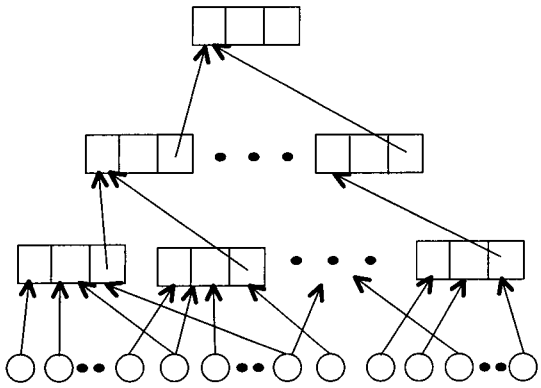
반면에 역할 그룹 인증서로 속성 인증서를 사용할 경우, (그림 3)과 같은 내용을 속성 인증서가 가지게 된다.

holder	attributes	extensions
pkc subject	역할 그룹 정보 (공백 가능)	역할 그룹 부가 정보

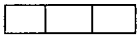
(그림 3) 속성 인증서의 내용

즉, 소유자(holder) 필드에 pkc(public key certificate, 공개키 인증서) subject를, 속성(attributes) 필드에 역할 그룹을, 확장(extensions) 필드에 추가정보를 가진다.

계층적 역할 그룹을 도입할 경우 속성 인증서는 (그림 4)와 같이 나무 구조를 이룬다.



(그림 4) 속성 인증서의 그룹 구조화

 : 속성 인증서

 : subject/holder

새로이 상위 노드에 정의되는 역할을 역할 그룹으로 명명한다. (이는 사용자(subject/holder) 그룹에 대해 역할을 부여하는 것과는 다르다.) 제안된 표준[4, 5]에서는 기술적으로 이러한 구조가 가능하도록 정의되어있으나 역할 적용시의 오버헤드로 이용이 제한되고 있다. 그러나 각 노드가 네트워크를 통해 고도로 분산되어 있는 경우 역할 적용시의 오버헤드에 비해 역할 갱신시에 얻는 성능 상의 이익이 더 크다. 역할 적용시의 오버헤드는 캐싱으로 극복할 수 있으므로, 역할 갱신시의 오버헤드를 줄이면 이는 고도의 분산된, 신뢰성이 낮은 네트워크 환경에서 매우 효과적이다.

역할 그룹의 도입은 그룹 구성원의 변화에 동적으로 대응하는 그룹 키 재구성(group rekeying)을 필요로 한다. 그룹 구성원이 갖는 그룹키 TEK_i에 대한 키 갱신은 그룹 크기의 동적 변화에 무관하게 상수의 시간에 이루어지도록 멀티캐스팅을 이용한다. 새로운 TEK_i'의 전송은 그룹원의 가입 또는 그룹이 합병될 경우(Member Join, Group Merge)와 그룹원의 탈퇴 또는 그룹이 분할될 경우(Member Leave, Group Partition)로 나눌 수 있으며 사용되는 멀티캐스트 패킷의 형태는 다음과 같다.

그룹원의 가입 또는 그룹이 합병될 경우의 그룹키 갱신 패킷 :

$Header;\ E_{TEK_i}[TEK_i']$

그룹원의 탈퇴 또는 그룹이 분할될 경우의 그룹키 갱신 패킷 :

$$Header;\ E_{PU_a}[TEK_i'];\ E_{PU_g}[TEK_i'];\ \cdots;$$
$$E_{PU_{ij}}[TEK_i'];\ \cdots;\ E_{PU_{im}}[TEK_i']$$

for $i = role\ group\ id$,

$1 \le j \le m$, m = 멤버의 개수

$PU_{ij} = public\ key$ for $member\ j$

$where\ member\ j \in role\ group\ i$

3. 역할 그룹 갱신 모델

(그림 4)와 같이 속성 인증서가 체인을 이룰 경우, 역할의 적용에 있어서 추가의 시간이 소요된다. 이를 개선하기 위하여 속성 인증서에 대하여 응집성 캐싱을 한다. 응집성 캐싱을 위하여 통신 패턴이 그룹 내에서 분석되며 응집성의 정도에 따라 캐싱의 정도가 결정된다. 응집성이 높을수록 캐싱의 확률이 높다. 관련된 캐싱의 방법 및 성능 분석은 [6]에 제시되어 있다. 본 논문에서는 역할의 갱신에 따른 속성 인증서 정보 갱신에 초점을 맞춘다.

갱신된 속성 인증서는 규모 확장성을 제공하는 멀티캐스트 통신을 통하여 전달되며, 그 기법은 다음과 같이 모델링된다.

◦ R : 역할 (r_i)의 수

◦ N : 최하위 역할 그룹의 최대 개수,

$$\binom{R}{1}+\binom{R}{2}+\binom{R}{3}+\cdots+\binom{R}{R-1}+\binom{R}{R}$$

$\binom{R}{1}$은 역할을 한 개 가지는 역할 그룹이고, $\binom{R}{R}$은 모든 역할을 포함하는 역할 그룹으로 transitive 한 경우이외에 실질적 의미는 거의 없으나 완전성을 갖추기 위하여 포함한다.

- k : 최하위 역할 그룹 속성 인증서의 최대 개수 = N
- n_i : 역할 그룹 i(i번째 역할 그룹)
- k_i : 역할 그룹 n_i에 관련된 역할 그룹 속성 인증서
- h : 트리의 높이 (루트의 레벨은 0이고 단말의 레벨은 $h-1$이다.)
- d_i : 역할 그룹 n_i의 차수

모든 중간노드의 차수를 $d_i=d$로 하면, $N=d^h$가 된다. N에 대해서 h를 어느 정도로 하는 것이 좋은가에 대해 알아보기 위해 다음 <표 1. 에 보인 바와 같이 R에 따른 $N'=\binom{R}{20}$의 값을 계산하였다. 이것으로 $N(>>N')$이 아주 큰 값을 가지게 되리라는 것을 알 수 있다. 그러므로 많은 역할을 그룹화하여 나무구조의 차수가 크도록 하는 것이 지나친 그룹의 생성을 막아 전체 시스템이 적정한 복잡성을 가지도록 한다. 나무구조의 차수에 따라 나무구조의 높이가 정해지며, 이에 대한 분석은 4장에서 보인다.

〈표 1〉 R에 따른 N'값의 변화

R	100	500	1000	5000	10000
N'	5.36E+20	2.67E+35	3.39E+41	3.77E+55	4.03E+61

레벨 $l(0 \le l \le h-1)$에서 역할 그룹 n_i의 속성 인증서 k_i의 갱신이 있다고 하자. 그러면 역할이 그룹화되어 있지 않는 경우, 속성 인증서는 전체 subject/holder의 수 만큼의 정보갱신이 필요하며 각각은 d^{h-l} 역할 관리자에게 전송되어야한다. 즉 속성 인증서의 수신자 $R(l)=d^{h-l}$이다. 반면에 역할이 그룹화되어있는 경우, 속성 인증서는 하위 역할 그룹의 수만큼의 정보갱신이 필요하며 각각은 d 역할 관리자에게 전송되어야 한다. 즉 속성 인증서의 수신자 $R(l)=d$이다.

레벨 l의 속성 인증서가 모든 $R(l)$에 보내는 전체 속성 인증서 전송횟수를 $M(l)$이라 하자. 그리고 하나의 $R(l)$ 수신자, r이 k_i를 전송받지 못할 패킷 손실율을 p라 하고, M_r은 r이 키 k_i를 성공적으로 받는데 필요한 속성 인증서 패킷 전송횟수라 하자. 패킷 손실 사건(event)는 서로 독립적이므로, 속성 인증서 전송횟수 M_r은 기하학적 분포를 가지며, 그에 따라 다음과 같이 계산할 수 있다.

$$P[M_r \le m] = 1-p^m, m \ge 1 \quad (1)$$

$$E(M_r) = 1/(1-p) \quad (2)$$

식 (1)은 m번 이내에 성공적으로 속성 인증서를 받을 확률이고, 식 (2)는 평균 속성 인증서(패킷) 전송횟수이다. 각각의 수신자에게 발생하는 패킷 손실 이벤트가 서로 독립적이므로, 수신자 $R(l)$ 전부가 m번 이내에 성공적으로 키를 받을 확률 $P[M(l) \le m]$은 식 (3)과 같다.

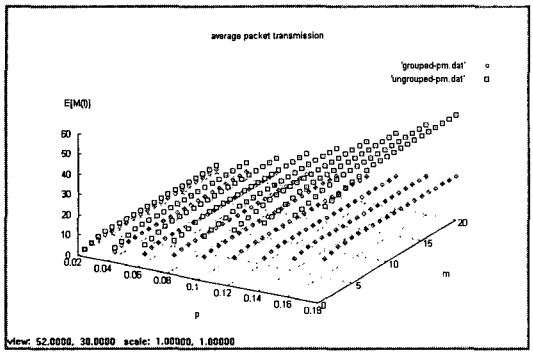
$$P[M(l) \le m] = \prod_{r=0}^{R(l)} P[M_r \le m] = (1-p^m)^{R(l)} \quad (3)$$

그러므로 평균 속성 인증서 패킷 전송횟수는 식 (4)와 같이 계산된다.

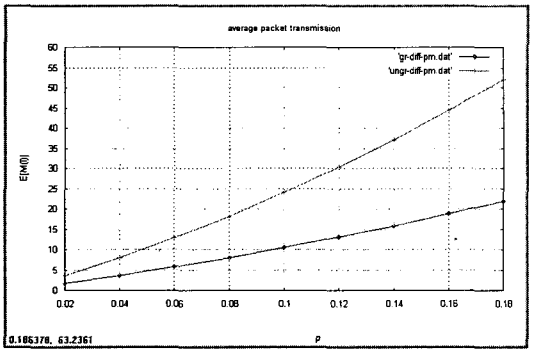
$$E[M(l)] = \prod_{m=1}^{\infty} P[M(l) \ge m] = \prod_{m=1}^{\infty} (1-(1-p^{m-1})^{R(l)}) \quad (4)$$

4. 성능 분석

식 (1)~식 (4)로부터 평균 속성 인증서 패킷 전송 회수 $E[M(l)]$을 구하여 성능 비교 및 분석을 한다.

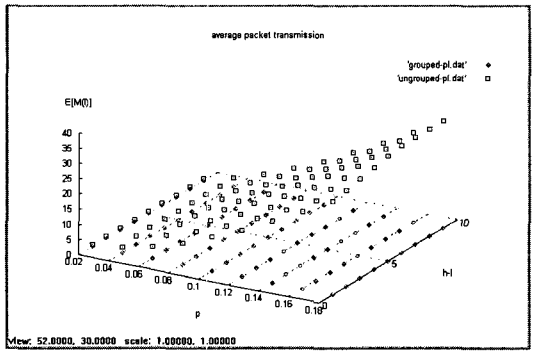


(그림 5) p와 m의 값의 변화에 따른 평균 속성 인증서 패킷 전송횟수

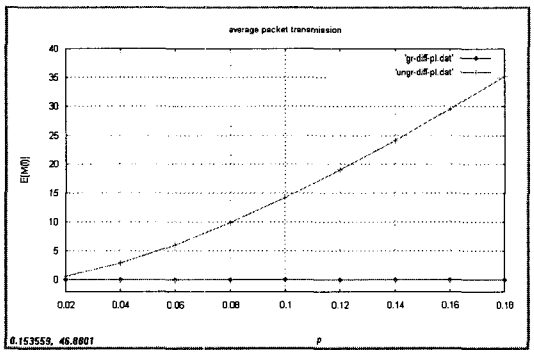


(그림 6) $m=20$인 경우 평균 속성 인증서 패킷 전송횟수

(그림 5)는 패킷 손실율 p와 임계치(threshold) m 값의 변화에 따른 평균 패킷 전송횟수 $E[M(l)]$를 나타낸다. m 값이 10을 넘어가면 $E[M(l)]$은 임계치에 근접하며 안정된 값을 가진다. $m=20$일 경우, p값의 변화에 따른 $E[M(l)]$ 의 값을 비교하면 (그림 6)과 같다. 그룹화 되지 않았을 경우(ungrouped-pm.dat) 평균 패킷 전송횟수 $E[M(l)]$이 급격히 커지나, 그룹화 되었을 경우(grouped-pm.dat) 완만한 증가를 보인다. 즉, $p=0.1$인 경우 50%, $p=0.16$인 경우 40% 정도로 평균 패킷 전송횟수가 줄어드는 성능 향상을 볼 수 있다.



(그림 7) p와 l의 변화에 따른 평균 속성 인증서 패킷 전송횟수



(그림 8) $(h-l)=5$일 경우 평균 속성 인증서 패킷 전송횟수

(그림 7)은 패킷 손실율 p와 전체 나무 구조 내에서 속성 인증서 갱신이 발생한 레벨의 레벨 차이 $(h-l)$에 따른 평균 속성 인증서 패킷 전송횟수를 나타낸다. 비교를 쉽게 볼 수 있도록 하기위해 레벨차이가 5일 경우에 대해 이차원 그래프를 그린 것이 (그림 8)이다. 그룹화 되지 않았을 경우(ungrouped-pl.dat) 평균 패킷 전송횟

수 $E[M(l)]$이 급격히 상승하나 그룹화 되어있을 경우(grouped-pl.dat) 평균 패킷 전송횟수가 현저히 낮을 뿐 아니라 패킷 전송횟수 증가의 변화가 미소함을 볼 수 있다. 그래서 $p=0.02$일 경우 40%, $p=0.1$일 경우 30%, $p=0.18$일 경우 26% 정도로 패킷 전송횟수가 점진적으로 줄어들어 네트워크 환경이 열악해 질수록(p가 커질수록) 성능상의 이익이 커짐을 알 수 있다.

5. 결 론

고도의 동적인 협업 환경에서는 접근제어를 다양한 수준에서 제공해야 자연적인 동적변화에 적응하여 최적의 접근제어 기능을 제공할 수 있다. 이를 위해서는 기 성립된 접근제어 관계에서 얻을 수 있는 특성 및 신뢰관계를 이용하는 것이 효율적이다. 이에 개별 역할에서 공통된 부분을 그룹화하고, 역할 그룹의 속성 인증서의 관계 구조 트리를 구성하여 분산된 환경에서 안전하고 효율적인 역할의 갱신과 분배를 달성한다. 규모 확장성을 위해 멀티캐스팅 패킷을 이용한 속성 인증서 분배를 하며, 그에 따른 네트워크 상의 패킷 손실율을 고려한 성능분석을 하였다. 역할 그룹을 두어 속성 인증서를 구조화하는 것이 역할의 갱신시에 발생하는 패킷 전송횟수를 크게 줄여 성능을 향상시킴을 정량적으로 보였다. 이는 유비쿼터스 환경과 같은 고도의 분산 컴퓨팅 환경에서 매우 유용한 것으로 사료된다.

참 고 문 헌

[1] R. Sandhu, V. Bhamidipati and Q. Munawer, "The ARBAC97 Model for Role-based Administration of Roles", *ACM Transactions on Information and System Security*, Vol.2, No.1, pp.105-135, 1999.

[2] David Ferraiolo, John F. Barkley and D. Richard Kuhn, "A Role-Based Access Control Model and Reference Implementation Within a Corporate Intranet", *ACM Transactions on Information and System Security*, Vol.2, No.1, pp.34-64, Feb. 1999.

[3] D. F. Ferraiolo, R. Sandhu, S. Bavrila, D. R. Kuhn and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control", *ACM Transactions on Information and System Security*, Vol.4, No.3, pp.224-274, 2001.

[4] ITI (Information Technology Industry Council), Role Based Access Control ITU/T(2001). Recommendation X.509 | ISO/IEC 9594-8, Information Technology Open Systems Interconnection-The Directory : Public-Key and Attribute Certificate Frameworks, 2003.

[5] S. Farrell and R. Housley, An Internet Attribute Certificate Profile for Authorization, IETF RFC 3281, 2002.

[6] 양수미, "그룹 키를 이용하는 응집성 권한 위임 캐쉉을 제공하는 역할 기반 접근 제어", 수원대학교 IT연구소 논문지, 2004. 11.

[7] H. Harney, U. Meth, A Colegrove and G. Gross, "GSAKMP", internet-draft : draft-ietf-msec-gsakmp-sec-06.txt, 2004.

[8] ISO/IEC 13568, International Standard : Information technology Z formal specification notation Syntax, type system and semantics, 2002.

[9] James B D Joshi, Elisa Bertino, Arif Ghafoor, "Temporal hierarchies and inheritance semantics for GTRBAC", Proceedings of the seventh ACM symposium on Access control models and technologies, Monterey,

California, USA, pp.74-83, 2002.

[10] Arthur Goldberg, Robert Buff, Andrew Schmitt, "Secure Web Server Performance Dramatically Improved by Caching SSL Session Keys", Workshop on Internet Server Performance held in conjunction with SIGMETRICS '98, 1998.

[11] Colin English, Paddy Nixon, Sotirios Terzis, Andrew McGetrtrick and Helen Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments", Workshop on Security in Ubiquitous Computing (UBICOMP 2002), Sep. 2002.

[12] Lalana Kagal, Tim Finin and Anupam Joshi, "Moving from Security to Distributed Trust in Ubiquitous Computing Environments", *IEEE Computer*, Dec. 2001. 12.

양 수 미

1985년 서울대학교 컴퓨터공학과 학사
1987년 서울대학교 컴퓨터공학과 석사
1997년 서울대학교 컴퓨터공학과 박사
1987년~1988년 한국전자통신연구원 연구원
1988년~2000년 한국통신 연구소 선임연구원
2000년~2001년 미국 UCLA 방문연구원
2002년~2004년 수원과학대학 컴퓨터정보과 교수
2004년~현재 수원대학교 인터넷정보공학과 교수