

An Efficient Role Specification Management Model for Highly Distributed Environments

Soomi Yang
 The University of Suwon
 Kyungki-do Hwasung-si Bongdam-eup Wau-ri san 2-2,
 445-743, Korea
 Email: smyang@suwon.ac.kr

Abstract—Highly distributed environments such as pervasive computing environments not having global or broad control, need another attribute certificate management technique. For an efficient role based access control using attribute certificate, we use a technique of structuring role specification certificates. It can provide more flexible and secure collaborating environments. The roles are grouped and made them into the relation tree. It can reduce management cost and overhead incurred when changing the specification of the role. Further we use caching of frequently used role specification certificate for better performance in case applying the role. Tree structured role specification results secure and efficient role renewing and distribution. Caching of role specification helps an application of role. In order to be scalable distribution of the role specification certificate, we use multicasting packets. Also, performance enhancement of structuring role specification certificates is quantified in the sense of taking into account of the packet loss. In the experimental section, it is shown that role updating and distribution are secured and efficient.

Index Terms—role specification, role based access control, multicast

I. INTRODUCTION

A role based access control using attribute certificates can provide more flexible and secure collaborating environments than that using only public key certificates. Use of attribute certificates can provide more flexible scheme by the use of role assignment certificates and role specification certificates.

American National Standards Institute, International Committee for Information Technology Standards (ANSI/INCITS) as ANSI INCITS 359-2004 is the information technology industry consensus standard for RBAC[1,2]. It reflects the importance of role based access control and shows that it makes the base of information technology.

Highly distributed collaborating environments such as pervasive network usually support the authorization of resources at varying levels of access. Furthermore, a significant characteristic of highly distributed environments is the need for interactions of highly collaborating entities to be secure. However, it could not have any central or global control. Due to the lack of central con-

trol, the autonomous entities form trust relations [3, 10, 12]. In the trust model, role based access control through the delegation of privileges to entities trusted via the use of certificates are used. They can be chained to represent recommendations and the propagation of trust.

For secure communication of highly distributed environments, we distribute the role specifications according to the levels of access. It accords with the characteristics of the distributed environments and sometimes is inevitable. In this paper, the concept of trust model is adopted. Our method is different from the privilege delegation [2] and it can be thought of as the distribution of privileges. In addition, we group roles, which is different from the typical methods which group subjects only [1,6,]. The property of the role group not only results in reduced network traffic but also reduces the overhead on the role manager. For scalability, we use multicast for distribution of role specifications. Our work is related to the technique used for group key management [8,9]. In the experimental section, it is shown that our method can enhance the performance.

The rest of this paper is organized as follows. In the next Section, we describe the secure role group model. In Section 3, the group communication model for updating and caching role specification is presented. In Section 4, the performance of our method is shown. In Section 5, we briefly describe related works. In section 6, we conclude.

II. SECURE ROLE GROUP MODEL

A secure role group is a extended version of the secure group [8, 9]. It is triple (G, P, R) where G is a finite and nonempty set of role groups ($Group_i$) and P is a finite and nonempty set of permissions. And R is a binary relation between G and P , $R \subset G \times P$, called the role group – permission relation of the secure role group. Role group G has permission p if and only if (g, p) is in R . Each secure role group has a trusted role group server responsible for generating and securely distributing permissions in P to users and roles in the role group. Specifically, the role group server knows the role group set G and the permission set P and maintains the role group-permission relation R .

The ITU-T X.509 Recommendation (ISO/IEC 9594-8) [2] and the IETF RFC 3281 [4] define AC (Attribute Certificate). Specific privileges are assigned to a role name through role specification certificate. The level of indirection enables the privileges assigned to a role to be updated, without impacting the certificates that assign roles to individuals. We make a chain of role specification certificates.

For structuring role specification certificates, we make role groups different to the subject groups. The structure of the role groups differs from that of the delegation of roles [2]. It gathers common roles and builds the trust structure. It forms the tree structure. The chain of role specification certificates can incur the overhead when a subject is going to use some privileges. The problem can be solved using coherent caching of role specification certificates [5]. Possible increase in increased administration and key management effort do not exceed the performance gain using attribute certificate [5]. In highly distributed environment, the distribution of the specifications of roles is inevitable. In this paper, caching of the role specification certificates is considered as well as updating of them. For the case that the role groups are distributed geographically and the role specifications are changed, the performance enhances. If the role group is not used, the role holder should possess all the role specifications. In this case, the application of the role can be done directly without following the role specification certificates. However, each subject should have all the role specification certificates, and the small memory devices commonly used in pervasive computing environment cannot afford it.

Attribute certificates or public key certificates can be used as role assignment certificates. When the public key certificates are used, the extensions field should have the information about role specification certificates.

On the other hand if the attribute certificates are used, the attribute certificate should have the contents as shown in Fig. 1.

holder	attributes	extensions
PKC subject	role information (possibly blank)	role specification certificate information

Figure 1. Contents of a role assignment certificate.

In other words holder field has PKC (public key certificate) subject and attribute field has roles (possibly it can be blank) and extensions field has the information for the role specification certificates. According to Fig. 1 role specification certificate should have the structures as shown in Fig. 2.

holder	attributes	extensions
role name	role information (possibly blank)	role specification certificate information

Figure 2. Contents of a role specification certificate.

For the role specification certificates shown in Fig. 2, extensions field can have another role specification certificate information repeatedly such as role name(*roleName*) or serial number(*serialNumber*). It forms the tree structure.

We call the node that corresponds to the role specification certificate having child role specification certificates as role group. If the nodes are distributed geographically, the performance enhancements gained when the chained role specifications should be changed are overwhelming. Furthermore the application overhead can be overcome by the use of caching. We are going to show the performance gains quantitatively in Section 4.

III. THE COMMUNICATION MODEL

Updated role specification certificates are delivered by the multicast communication. The distribution of updated role specification certificates of our method can be modeled similarly to [12] as following:

- R : the number of roles
- G : the number of the lowest level role groups
- G_{max} : the maximum number of the lowest level role groups, $\sum_{i=1}^R R C_i$
- S : the number of the lowest level role specification certificates
- S_{max} : the maximum number of the lowest level role specification certificates, $S_{max} = G_{max}$
- g_i : role group i
- s_i : role specification certificate related to role group g_i
- h : height of the tree structure starting from 0
- d_i : degree of role group g_i

If d_i equals to d for all i then G equals to d^h . In general, the roles are included in not all of role groups. The roles are created on its own behalf. They are not normalized. Thus, excessive role group creation should be avoided by determining the proper value of h . If the roles are not grouped, s_i needs to be transmitted to d^{h-1} members. From the viewpoint of the reliable delivery, a role specification certificate s_i at level l of the tree structure has to be delivered to $W(l) = d^{h-l}$ receivers. If the roles are grouped, s_i needs to be transmitted to d members. Thus, it has to be delivered to $W(l) = d$ receivers. Let $F(l)$ be the frequency of the transmission of a role specification certificate s_i in order to be successfully delivered to all $W(l)$ receivers.

The probability that one of these $W(l)$ receivers (say w) will not receive the updated role specification if it is transmitted once is equal to the probability of packet loss, p , for that receiver. Let F_w be the frequency of role

specification transmissions necessary for receiver w to successfully receive the role specification certificate. Since all the packet loss events for receiver w , including replicated packet and retransmissions, are mutually independent, F_w is geometrically distributed as in [8, 9]. Thus,

$$P[F_w = f] = p^{f-1}(1-p) \quad (1)$$

$$P[F_w \leq f] = 1 - p^f, f \geq 1 \quad (2)$$

From Equation (1), we can induce average expected frequency as following.

$$E(F_w) = \sum_{f=1}^{\infty} mP[F_w = f] = 1/(1-p) \quad (3)$$

Equation (1) represents the probability that the role specification certificate is successfully delivered on f try after suffering $f-1$ times failed transmission. So the Equation (2) represents the probability that the role specification certificate is delivered successfully within f packet transmissions. Equation (3) represents the expected number of packet transmission. Since lost packet events at different receivers are independent each other, the probability $P[F(l) \leq f]$ that all the $W(l)$ receivers will receive the packet within f transmissions is as shown in Equation (4).

$$p[F(l) \leq f] = \prod_{w=1}^{W(l)} P[F_w \leq f] = (1 - p^f)^{W(l)} \quad (4)$$

The average expected frequency of the role specification packet transmission can be computed as following:

$$E[F(l)] = \sum_{f=1}^{\infty} P[F(l) \geq f] = \sum_{f=1}^{\infty} (1 - (1 - p^{f-1})^{W(l)}) \quad (5)$$

We can compute $E[F(l)]$ numerically using Equation (5) by truncating the summation when the f th value falls below the threshold.

A. Caching

For an application of the role specification certificate, $2^{*(h-1)}$ packets should be successfully transmitted if the requested role specification is located at level l of the tree. It forms a path through the role specification tree from a requesting node to a node having requested role specification certificate. In other words, $h-1$ packet transmission for a delivery of request and another $h-1$ packet transmission for a delivery of role specification certificate are required.

To improve the application of the role specification, caching scheme can be adopted. Let $G(l)$ be the frequency of the transmission of packets for the successful delivery of a role specification certificate S_i to a requesting node. If the probability of having cached role specification certificate is q , the average expected frequency of the role specification packet transmission can be computed as following from the similar induction of Equation (1) through (5).

$$\begin{aligned} E[G(l)] &= (1-q) \sum_{f=1}^{\infty} P[G(l) \geq f] \\ &= (1-q) \sum_{f=1}^{\infty} (1 - (1 - p^{f-1})^{2^{(h-l)}}) \quad (6) \end{aligned}$$

A cached role specification does not need any packet transmission. It holds some space of a requesting device. Instead of caching role specification, we can reduce the time needed for acquiring the user's role specification by lowering the level of role specification. Lowering the level of role specification means amalgamation of role specifications. Lowered level of role specification reduces the packet transmission and saves the memory of the requesting device through the help of more complex management. In the following performance evaluation, we only consider the caching. More complex management technique including role specification compaction and normalization will be considered in further research.

B. Normalization

For global space reduction, we can normalize the role specification. In normalized role specification tree, role specification should appear only in one certificate. Then $G_{norm} = S$, $h = G_{norm} - 1 = S - 1$ and $d = 2$. Therefore the number of certificates in level l is $G_{norm} C_{h+1-l} = 2^l$. Thus the total number of certificates can be induced to $\sum_{i=1}^{G_{norm}} G_{norm} C_i$. It can include unused role group. However it generally significantly reduces the space compared to the space used for naturally evolving and diminishing role specifications without any regulation. In normalized role specification environment, if there is no redundant specification, and when the roles are not grouped, a role specification certificate S_i at level l of the tree structure has to be delivered to $W(l) = d^{h-l} = 2^{h-l}$ receivers. If the roles are grouped, S_i needs to be transmitted to d members. Thus, it has to be delivered to $W(l) = d = 2$ receivers. Thus it reduces management cost and overhead incurred when changing the specification of the role as shown in Table 1.

TABLE I.
THE NUMBER OF PACKET TRANSMISSIONS FOR CHANGING THE SPECIFICATION OF THE ROLE.

	un-normalized		normalized	
	ungrouped	grouped	ungrouped	grouped
$f = 10$ $p = 0.1$	2.54	1.39	1.66	1.21
$f = 200$ $p = 0.9$	45.53	20.27	26.30	14.74

* $d=4, h=3$

Normalization improves space utilization. However it increases path length and incurs more packet transmis-

sion when the subject is going to apply the role specifications. Therefore the degree of normalization should be adapted to the individual environment characteristics.

IV. PERFORMANCE EVALUATION

From Equation (1) through (6), we can measure the expected number of packet transmission, $E[F(l)]$ and $E[G(l)]$, for the performance comparison. First, to identify the effect of role grouping, we examine the average role specification packet transmission, $E[F(l)]$, for the various values of packet loss p and threshold f with $d=5, h=7$ and $l=4$. In Fig. 3, $E[F(l)]$ becomes stable when f becomes greater than 20 for role grouped case and 50 for role un-grouped case. Let's calculate the impact of p on $E[F(l)]$ when $f=50$ for two cases; one is when roles are not grouped and the other is when roles are grouped. For the role grouped case, $E[F(l)]$ results in higher value than the role un-grouped case. When p is 0.1, $E[F(l)]$ is reduced by 50% and when $p=0.3$, by 45%. When the quality of network is more inferior (so p is greater), the performance obtained through role grouping improves.

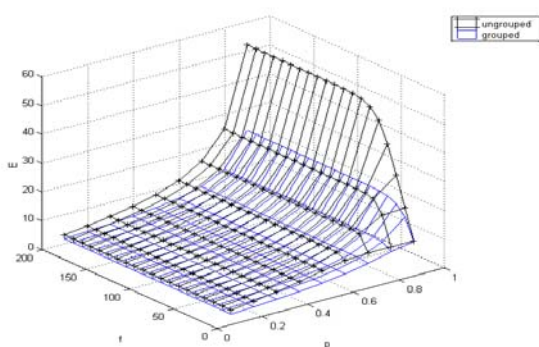


Figure 3. A comparison of role grouped case and role un-grouped case.

For each given caching ratio q , we can inspect the effects to the average packet transmission. Fig. 4 shows the frequency variations by packet loss p and caching ratio q with $f=100$. When the packet loss is small, the difference is small. However, as the packet loss gets bigger, it suffers more increasing packet transmission.

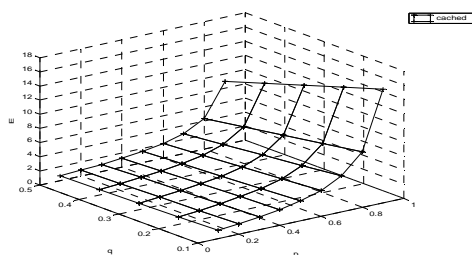


Figure 4. The expected packet transmission when role specifications are cached.

Fig. 5 shows the plot of the expected packet transmission $E[F(l)]$ and $E[G(l)]$ for packet loss p and the caching ratio q . Fig. 5 shows the greater increase in $E[F(l)]$ where the roles are grouped than in $E[G(l)]$ where the roles are grouped and the role specifications are cached. If we take a specific sample case, Table 2 shows portions the caching occupies when the requesting role specifications forms 30 percent. From the values given in Table 1 we can see that total number of the packet transmission should be greatly decreased when the role specifications are cached. However if the nodes are distributed geographically and the packet loss is more often, the performance enhancements gained when the role specifications should be changed are overwhelming.

TABLE II.
RATIO OF THE NUMBER OF PACKET TRANSMISSIONS FOR THE ROLE CACHED CASE BY THE ROLE GROUPED CASE

	q = 0.1	q = 0.5
p = 0.1	0.80	0.45
p = 0.9	0.73	0.40

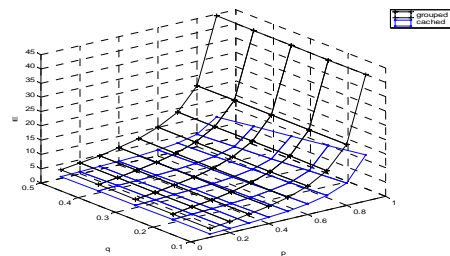


Figure 5. A comparison of the expected packet transmission as a function of p and q .

V. RELATED WORK

The ITU-T X.509 Recommendation (ISO/IEC 9594-8)[2] and the IETF RFC 3281 [4] define the architecture that make our proposal possible. However because of the overhead incurred when privileges are applied its use is not recommended. But if the nodes are distributed geographically, the performance enhancements gained when the role specifications should be changed are overwhelming. Furthermore the application overhead can be overcome somewhat by the use of caching as we have shown in previous section. Thus our technique makes use of it for the pervasive computing environments.

There have been many different proposals in the area of role based access control in pervasive computing. [3] and [7] build delegation chains between trusted parties. [7] uses delegate messages signed by their private keys constructed in simplified PKI (Public Key Infrastructure).

[10] makes use of capability for role definition in its role based access control instead of attribute certificate of our method.

[11] establishes access control manager which grants or denies permission having coordination of the trust calculator and cost analyzer. In their SECURE framework, roles are specified in role credential similar to attribute certificate.

Our novel technique utilizing attribute certificates and structuring role specifications conforms to the standard and can be adapted to existing schemes in a seamless way.

VI. CONCLUSION

For optimized access control, the use of the established characteristics and trust relation is efficient and natural. Thus, we adopt the characteristics of highly distributed computing environments and the useful trust model. As an efficient access control using attribute certificate, we use the technique of structuring role specification certificates and reinforce it through caching them. It can reduce the management cost and overhead incurred when changing and applying the specification of the role. Especially, highly distributed computing environments such as pervasive computing which cannot have global or broad control need flexible attribute certificate management technique. Even though, the role specification certificate itself reduces management cost, the structuring of role specification is needed in order to get flexibility with better performance. We grouped roles, made the role group relation tree, and showed the model description. It provides the secure and efficient role updating and the distribution. For scalable role specification certificate distribution, we used multicasting packets. The performance enhancements are quantified with taking into account the packet loss, too. Also, we showed that our scalable access control technique outperformed the existing access control techniques.

REFERENCES

- [1] 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*, 4(3), (2001) 224-274
- [2] ITI (Information Technology Industry Council), Role Based Access Control ITU/T. Recommendation X.509 | ISO/IEC 9594-8, *Information Technology Open Systems Interconnection-The Directory: Public-Key and Attribute Certificate Frameworks* (2003)
- [3] Colin English, Paddy Nixon, Sotirios Terzis, Andrew McGettrick and Helen Lowe: *Dynamic Trust Models for Ubiquitous Computing Environments*, Workshop on Security in Ubiquitous Computing (UBICOMP 2002)
- [4] S. Farrell and R. Housley, An Internet Attribute Certificate Profile for Authorization, IETF RFC 3281, (2002)
- [5] S. Yang: Role Based Access Control Supporting Coherent Caching of Privilege Delegation Which Utilizes Group Key, *The Journal of Suwon Information Technology*, Vol. 3 (2004)
- [6] 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 (2002) 74 - 83
- [7] Lalana Kagal, Jeffrey L Undercoffer, Filip Perich, Anupam Joshi, Tim Finin, A Security Architecture Based on Trust Management for Pervasive Computing Systems, *Grace Hopper Celebration of Women in Computing* (2002)
- [8] Sanjeev Setia, Sencun Zhu and Sushil Jajodia, A Comparative Performance Analysis of Reliable Group Rekey Transport Protocols for Secure Multicast, *proc. of the Performance* (2002)
- [9] Sandro Rafaeli, David Hutchison, A Survey of Key Management for Secure Group Communication, *ACM Computing Surveys*, Vol. 35, No. 3 (2003)
- [10] Giacomo Cabri, Luca Ferrari, Franco Zambonelli, Role-based Approaches for Engineering Interactions in Large-scale Multi-Agent Systems, *Software Engineering for Large-Scale Multi-Agent Systems II : Research Issues and Practical Applications* (2003)
- [11] Nathan Dimmock, Andras Belokosztolszki, David Eysers, Using Trust and Risk in Role-Based Access Control Policies, *9th ACM Symp. on Access Control Models and Technologies(SACMAT)* (2004)
- [12] Soomi Yang, An Efficient Access Control Model for Highly Distributed Computing Environment, *Distributed Computing – IWDC 2005 (LNCS 3741, Springer Verlag)* (2005)

Soomi Yang received the B.S., M.S. and Ph.D. degrees in computer engineering from Seoul National University of Seoul, Korea, in 1985, 1987 and 1997 respectively.

From 1988 to 2000, she was a researcher at Korea Telecom Research Center where she worked on telecommunication network, internet and information security. From 2000 to 2001, she was a visiting scholar at UCLA, USA. From 2002 to 2004, she was a faculty of the Suwon Science College. Since 2004, she has been on the Faculty of the University of Suwon, Korea, where she is a professor of computer sciences. Her research interests in information security include access control, network security, and secure system software.