Enforcing Access Control Using Risk Assessment

Nguyen Ngoc Diep[1], Le Xuan Hung[1], Yonil Zhung[1],
Sungyoung Lee[1], Young-Koo Lee[1], and Heejo Lee[2]
[1]*Dept. of Computer Engineering, Kyung Hee University, Korea*
[2]*Dept. of Computer Science and Engineering, Korea University, Korea*
{nndiep,lxhung,zhungs,sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr, heejo@korea.ac.kr

Abstract

Context-based access control is an emerging approach for modeling adaptive solution, making access control management more flexible and powerful. But in the ubiquitous environment, this approach is not enough for many emerging security vulnerabilities. Thus, improving current access control mechanisms is still necessary. Risk is an effective tool used for decision-making in economics. In this paper, we design a new model for risk assessment in ubiquitous environment and use risk as a key component in decision-making process in our access control model. This solution makes access control management more dynamic and precise.

1. Introduction

Ubiquitous computing integrates computation into the environment, rather than having computers which are distinct objects. Its unique features make it different from other computer science domains. They are ubiquity, invisibility, sensing, heterogeneous and resource-constrained. With these features, ubiquitous environment is not only the virtual world as traditional computing environment but the strong combined environment of virtual and physical world. Therefore, security problems are much more complex in ubiquitous computing compared with traditional environment.

Access control is concerned with limiting the activity of legitimate users who have been successfully authenticated, and is the process of ensuring that every access to a system and its resources is controlled and only those access that are authorized can take place. There are three basic components in an access control system: the subjects, the targets and the rules which specify the ways in which the subjects can access the targets.

Traditional access control mechanisms are context insensitive. They require a complex and static authentication infrastructure. Current research about access control is mostly based on the context and role [1]. Some recent research used trust as the fundamental component [2, 3, 4]. Some combine trust with risk to create a stronger security service to support peer-to-peer environment [4, 9].

In one of the most influential textbooks in decision theory, the term risk is defined as follows [10]*:*

Risk if each action leads to one of a set of possible specific outcomes, each outcome occurring with a known probability. The probabilities are assumed to be known to the decision maker.

Risk assessment is an effective tool using in decision-making and is an important factor in economics. When applying it to security area, especially access control, there will be some difficulties due to the differences between the two areas. But we believe that with risk, we can create a flexible, adaptive, powerful access control mechanism.

In this paper, we propose an approach for access control management based on risk assessment and context. We use the risk assessment to assist the decision-making process at access control manager. They both use context to make the system more flexible and powerful.

Rest of the paper is organized as follows: In section 2, we briefly introduce the related works. The architecture of the system is described in section 3. Section 4 is our design of risk assessment mechanism, how it works with the context and other parameters. Section 5 presents a case study for our approach. Section 6 consists of future work and conclusion.

2. Related work

In this section, we present a briefly summary of related work. We will mention some aspects of context, access control mechanism and risk

Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07)
0-7695-2768-X/07 $20.00 © 2007 IEEE

assessment. We summarize the effort of these directions and then highlight the significance of our particular work.

Role based access control (RBAC) is an alternative to traditional discretionary (DAC) and mandatory access control (MAC). In RBAC, users are assigned roles and roles are assigned permissions. Recently RBAC was found to be the most attractive solution for providing security features in different distributed computing infrastructure. Although RBAC models vary from very simple to pretty complex, they all share the same basic structure of subject, role and privilege. Other important factors like context information are not considered. Thus, in a new environment like ubiquitous environment, RBAC can not afford to fulfill the need of security. And finally, several approaches have been presented in literature to address the problem due to dynamic content and context-awareness of ubiquitous environment.

Michael J. Covington et al. [11] have proposed the Generalized Role Based Access Control (GRBAC) model. In this model, they extend the traditional RBAC by applying the roles to all the entities in a system. (In RBAC, the role concept is only used for subjects). By defining three types of roles, i.e., Subject roles, Environment roles, and Object roles, GRBAC uses context information as a factor in making access decisions.

Guangsen Zhang et al. [12] also uses context parameters in their dynamic role-based access control model with two key ideas: (1) A user‘s access privileges must change when the user’s context changes. (2) A resource must adjust its access permission when its system information (e.g., network bandwidth, CPU usage, memory usage) changes.

These two above papers really make the access control dynamic and flexible but the decision-making process is not as powerful and precise as that in our model using risk. They did not consider the aspect of security in making-decision process and the impact of security problems on the system.

The paper of Nathan Dimmock et al. [9] uses the concept of outcome to calculate cost for each outcome and risk value but they do not consider context for risk assessment. So it loses the flexibility characteristic in evaluating risk. They did not consider risk as an important factor in their access control mechanism and they did not use risk directly in making decision.

We can say that, using combination of risk and context for making decision creates a powerful, flexible access control model. Especially, we use context parameters as the inputs in the risk assessment process and the result is improvement of preciseness in each access control decision.

3. Access Control Model with risk assessment

3.1. The access control framework

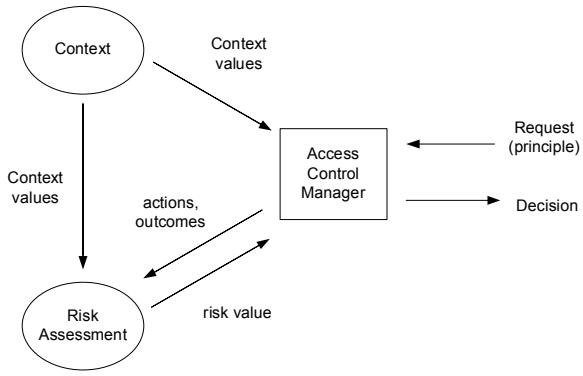

Figure 1. Access Control Framework

This section presents the framework of our access control system. There are three modules in the system as in figure 1. In which, the access control manager is main module. It receives requests from requesters, analyses them, collects other parameters and sends the data to risk assessment module. After that, it makes decisions for each request based on risk value from risk assessment module.

Risk assessment is a key module in the framework. It calculates risk value based on the input data from access control manager and context data from context module.

Context module has responsibility of collecting parameters from users and environment to support other modules. In this paper, we do not mention how to aggregate context data from users and environment. Context can be obtained from CAMUS Server in [13].

3.2. Access Control Model

A request from principle p to perform an action is submitted to the access control manager. The access control manager looks up relevant outcomes that may occur due to this action and query risk assessment module for calculating risk value after sending it necessary parameters. The risk assessment module, after calculating cost of outcomes in term of availability, confidentiality, and integrity based on context of principle, environment and resource, evaluates risk value of the action. The decision is made at access control manager based on risk value from risk assessment module. The risk value is compared with the threshold, and then access control manager returns

the decision. The period during the action acts is called session.

The model has following factors:
- **Principle** (p): users or processes
- **Set of action** (A) available for principle
- **Set of outcome** (O): those are consequences of action and the results are loss of confidentiality, availability, and integrity.
- **Set of context** (s): consists of principle, environment and resource context. For example, they can be time (night, daytime…), location (in-building, in-office, outside), network state, state of resource.
- **Consequence function**, c(o), that shows the cost of each outcome in the specific state.
- **Risk function** RV(o,a): expressing the risk of the action in the current state. The system bases on this value to work out the decision
- **Threshold**: we have a threshold to compare with risk value in order to making decision.

4. Estimating Risk in Ubiquitous Computing

Our mathematical model of risk bases on three basic units. They are loss of availability, loss of confidentiality and loss of integrity. The reason is the objectives of security, as we know, are availability, confidentiality and integrity.

When we make decisions, we try to obtain as good an outcome as possible. One way to express the value pattern is as a relation between elements. Another way is to assign numerical values to each element. This is numerical representation. And in this paper, we use the later method to combine context with risk value.

There are many factors that affect our risk estimation process. For each action, the risk value depends on the outcomes. And if the cost for the outcome (due to the action) is high, the risk is high. Risk also depends on current context parameters. For example, in the condition of low internet connection speed, it easily loses the session of an ftp connection. It means we lose the availability. Or if we have wireless connection, we are easily hacked.

The property of the resources in the action also has an important role in evaluating risk. But the risk it creates depends on the sort of action and the context of the outcome. Assuming that, the risk created from the action such as deletion of a big video file is less than the risk of copying a big video file in term of loss of availability.

From those claims, we come up with our evaluating process.

4.1. Cost of outcome

We have inputs, consisting of the action and list of consequence outcomes of the action. In fact, each outcome may occur in some specific contexts, consisting of principle context, environment context and resource context. Principle context is a set of information that references to the principle, such as preferences and rights of user. Environment context is a set of information collected from the user's environment and the application environment. Resource context is considered as properties of the resource and the state of it. Assuming that value of context parameters of all kind of context can be retrieved from context module. We base on these values to calculate risk for each outcome.

In the aspect of principle context and environment context, we have some parameters including time, location, state of network… They can be defined, for example: time (rush hours, day time, night time), location (in-room, in building, outside), network state (normal, abnormal). For each action, these parameters create different risk value in term of availability, integrity, confidentiality.

The effect of the resource to risk value depends on properties of resource and we should have some pre-defined threshold. For example, if the size of a video file is more than 100MB and the action is downloading, risk value in term of loss of availability is cost1.

Risk is often evaluated based on the probability of the threat and the potential impact.

We have some definitions:

- Action a_i is an action in set of action A (available for the principle), $i \in N$
- $o_{a_i,j}$ is an outcome in set of outcome O of action a_i, $j \in N$
- $lo\_a_{a_i,j}$ is cost of outcome j of action a_i in term of availability
- $lo\_i_{a_i,j}$ is cost of outcome j of action a_i in term of integrity
- $lo\_c_{a_i,j}$ is cost of outcome j of action a_i in term of confidentiality
- s_k: consisting of a set of context parameter, $k \in N$
- $f_{o_{a_i,j},s_k}$ is the probability of outcome $o_{a_i,j}$ in context s_k Then, cost of the outcome in term of availability is:

$$c\_a_{o_{a_i,j}} = lo\_a_{a_i,j} \times (\sum_k f_{o_{a_i,j},s_k}) \qquad (1)$$

Cost of the outcome in term of integrity is:

$$c\_i_{o_{a_i,j}} = lo\_i_{a_i,j} \times (\sum_k f_{o_{a_i,j},s_k}) \quad \textbf{(2)}$$

Cost of the outcome in term of confidentiality is:

$$c\_c_{o_{a_i,j}} = lo\_c_{a_i,j} \times (\sum_k f_{o_{a_i,j},s_k}) \quad \textbf{(3)}$$

In this case, s_k exists if and only if all required context parameters exist.

4.2. Cost of action

Within an action, the importance of each outcome is different. An outcome if occur might lead to a great loss, but another does just a little. So, we give each outcome a value called weight of outcome.

Cost of an action is a weighted arithmetic mean of all outcomes of the action. Similarly, we can calculate cost of each action in term of availability, integrity and confidentiality one after another.

For availability:

$$\cos t(a_i, "availability") =$$

$$RV\_A_i = \frac{\sum_j \left(w_{o_{a_i,j}} \times c\_a_{o_{a_i,j}} \right)}{\sum_j w_{o_{a_i,j}}} \quad \textbf{(4)}$$

For integrity:

$$\cos t(a_i, "integrity") =$$

$$RV\_I_i = \frac{\sum_j \left(w_{o_{a_i,j}} \times c\_i_{o_{a_i,j}} \right)}{\sum_j w_{o_{a_i,j}}} \quad \textbf{(5)}$$

For confidentiality:

$$\cos t(a_i, "confidentiality") =$$

$$RV\_C_i = \frac{\sum_j \left(w_{o_{a_i,j}} \times c\_c_{o_{a_i,j}} \right)}{\sum_j w_{o_{a_i,j}}} \quad \textbf{(6)}$$

where $w_{o_{a_i},j} \in N$ and they can be adjusted to a suitable value if more weight is to be given to a specific metric.

4.3. Risk value evaluation

In fact, with each service, we consider the importance of each element different. For example, availability evaluation should be given more importance over the others in a case of downloading files.

So, the risk value of an action is defined as a weighted arithmetic mean of its risk value of availability, confidentiality and integrity. Precisely, it can be calculated as:

$$RV = \frac{w_1 RV\_A_i + w_2 RV\_I_i + w_3 RV\_C_i}{w_1 + w_2 + w_3} \quad \textbf{(7)}$$

where $w_i \in N, \mathrm{i} = 1,2,3$ and they can be adjusted to a suitable value if more weight is given to a specific metric.

5. A case study – Access control management in a hospital

Assuming that, we have an access control system to manage access to patient‘s records in a hospital. Data is stored in database and can be accessed through remote terminal.

The records can be text, video, image or sound format and it has some properties like size of record, format, encrypted or not, only updated in a predefined time, etc.

Hospital staff who wants to access patient’s health records first login to the system as a member of the staff. Depending on his role, he can do some permitted actions on some corresponding records. The action he wants to do, for example, is viewing one record (or modifying some information and updating). The action “viewing record” has some outcomes such as unavailable, service corrupted, leaking information ... These outcomes in a particular context lead to loss of availability, loss of integrity or loss of confidentiality. The number of states is limited and risk value for each outcome in case of each kind of losses can be specified. We can see the example in table 1.

Applying the formulas in previous part, we can evaluate cost for each outcome of each action and risk value of the action.

Table 1. Outcomes and risk value for each action.

Action	Outcomes	Risk context /Probability	Risk value		
			Availability	Integrity	Confidentiality
View record	- Unavailable	- Record too big /f1 - Transaction session is nearly full /f2	*Cost1*	*Cost2*	*Cost3*
	- Leaking information	- Data unencrypted /f3 -Connection is not secured /f4	*Cost4*	*Cost5*	*Cost6*
	- Service corrupted	-Connection is lost /f5	*Cost7*	*Cost8*	*Cost9*
Modify record	- Lose information - Can not update	- Connection lost /f6 - Server busy, corrupted /f7	*Cost10* *Cost13*	*Coss11* *Cost14*	*Cost12* *Cost15*
Delete record	- Lose information - Can not delete	- Do not have backup /f8 - Not in right time /f9	*Cost16* *Cost19*	*Cost17* *Cost20*	*Cost18* *Cost21*

For example, we need to calculate risk value for action "View record". Look at the table 1, we easily find the cost of each outcome.

Cost of outcome "Unavailable" in term of availability is:

$$c\_a_{1a} = c\_a_{Unavailability}("Avalability") = \cos t1 \times (f1 + f2)$$

Cost of outcome "Unavailable" in term of integrity is:

$$c\_a_{1i} = c\_a_{Unavailability}("Integrity") = \cos t2 \times (f1 + f2)$$

Cost of outcome "Unavailable" in term of confidentiality is:

$$c\_a_{1c} = c\_a_{Unavailability}("Confidentiality") = \cos t3 \times (f1 + f2)$$

Similarly, we calculate cost of two other outcomes of action "View record":

$c\_a_{2a}, c\_a_{2i}, c\_a_{2c}, c\_a_{3a}, c\_a_{3i}, c\_a_{3c}$.

Then, we can calculate the risk for loss of availability of action "View record":

$$RV\_A = \frac{w_{o1} \times c\_a_{1a} + w_{o2} \times c\_a_{2a} + w_{o3} \times c\_a_{3a}}{w_{o1} + w_{o2} + w_{o3}}$$

where w_{o1}, w_{o2}, w_{o3} are weight of three outcomes "Unavailable", "Leaking information", "Service corrupted" of action "View record".

We also have value RV_I, RV_C by the same way. w_1, w_2, w_3 are weights of RV_A, RV_I and RV_C. So,

we can calculate the risk value of action "View record". The final risk value is the mean value:

$$RV = \frac{w_1 RV\_A + w_2 RV\_I + w_3 RV\_C}{w_1 + w_2 + w_3}$$

where w_i , i = 1,2,3 is predefined by administrator.

The risk value is compared with a threshold, and the decision is "OK" if $RV < threshold$.

6. Conclusion and future work

In this work, we have investigated how to apply risk to access control and propose an access control model with risk assessment. This model is a dynamic in management and flexible in handling access control. It provides a precise way of making decision because of taking context into risk assessment. We gather all useful information from the environment, evaluating them in security view. So we can reduce impacts of loss of security to the system. We have further demonstrated how this model can be applied to manage access control in a hospital and explored it in manner of ubiquitous computing.

We also design a risk assessment model that closely combined with context parameters and we believe it is lightweight and efficient when used in decision-making process.

The above work is still in infancy state. In future work, we need to consider more parameters and factors that effect to risk assessment process. One of them can be risk in authentication phase. We also need to consider about automatically handling session and adaptive features. We believe decision-making should be done during the working period of the activity, whenever the context changes into another state. Handling session also need to be flexible in order to support the best service for the users. And we think the efficiency of the system will be improved if we can automatically update the cost of outcomes of the actions, the threshold value in making decision process and the detailed information of current network state based on evidence gathered from the context

framework, maybe through some intrusion detection systems or network management systems.

Implementation this model in practice is little complicated. There have no standard about evaluating risk value for each state of the environment, for each outcome of action. So that, this mechanism has maximum efficiency only if we have experience system administrator who can give reasonable value for each element, each factor in early state of risk assessment process.

7. Acknowledge

This work is partially supported by the Ministry of Commerce, Industry& Energy, Korea.

8. References

[1] R.J. Hulsebosch , A.H. Salden, M.S. Bargh, P.W.G. Ebben, and J. Reitsma, "Context Sensitive Access Control", *In proceedings of the tenth ACM symposium on Access control models and technologies*, Stockholm, Sweden, 2005.

[2] Lalana Kagal, Tim Finin, and Anupam Joshi, "Trust-based security in pervasive computing environments", *IEEE Computer*, December 2001.

[3] V. Cahill, B. Shand, and E.Gray et al., "Using Trust for Secure Collaboration in Uncertain Environments", *Pervasive Computing*, July-September 2003, vol. 2, no. 3, pp. 52-61.

[4] Nathan Dimmock, Jean Bacon, David Ingram, and Ken Moody, "Risk models for trust-based access control (TBAC)", *In Proceedings of the Third Annual Conference on Trust Management (iTrust 2005)*, volume 3477 of LNCS. Springer-Verlag, May 2005.

[5] Peter Chapin, Christian Skalka, and X. Sean Wang, "Risk assessment in distributed authorization", *Proceedings of the 2005 ACM workshop on Formal methods in security engineering*, Fairfax, VA, USA, November 11-11, 2005.

[6] Hassan Jameel, Le Xuan Hung, Umar Kalim, Ali Sajjad, Sungyoung Lee, and Young-Koo Lee, "A Trust Model for Ubiquitous Systems based on Vectors of Trust Values", *Seventh IEEE International Symposium on Multimedia (ISM'05)*, 2005, ism, pp. 674-679 .

[7] Y. Chen, C. Jensen, E. Gray, V. Cahill and J-M Seigneur, "A General Risk Assessment of Security in Pervasive Computing", *Technical Report TCD-CS-2003-45, Department of Computer Science*, Trinity College Dublin, 6 November 2003.

[8] Y. Chen, C. Jensen, E. Gray, and J-M. Seigneur, "Risk Probability Estimating Based on Clustering", *In Proceedings of the 4th IEEE Anual Information Assurance Workshop*, West Point, New York, U.S.A., June 2003.

[9] Nathan Dimmock and Andrá Belokosztolszki and David David Eyers, Jean Bacon, Ken Moody, "Using Trust and Risk in Role-Based Access Control Policies", *Proceedings of Symposium on Access Control Models and Technologies*, 2004.

[10] Sven Ove Hansson, *Decision Theory: A Brief Introduction*, Department of Philosophy and the History of Technology, Royal Institute of Technology (KTH), Stockholm, 1994.

[11] M. J. Moyer M. J. Covington and M. Ahamad, "Generalized role-based access control for securing future applications", *In 23rd National Information Systems Security Conference,* (NISSC 2000), Baltimore, Md, USA, October 2000.

[12] Zhang, G. and Parashar, M., "Context-Aware Dynamic Access Control for Pervasive Applications", *In Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2004)*, *Western MultiConference (WMC)*, San Diego, CA, USA, January 2004.

[13] Hung Q. Ngo, Anjum Shehzad, and S.Y.Lee, "Developing Context-Aware Ubiquitous Computing Systems with a Unified Middleware Framework", *The International Conference on Embedded and Ubiquitous Computing (EUC04)*, Aizu-Wakamatsu City, Japan, 25-27 August, 2004.