Contextual Risk-based Access Control

Nguyen Ngoc Diep, Sungyoung Lee, Young-Koo Lee
Dept. of Computer Engineering
Kyung Hee University
Suwon, Korea

HeeJo Lee
Dept. of Computer Science and Engineering
Korea University
Seoul, Korea

Abstract - *Context-based access control is an emerging approach for modeling adaptive solution, making access control management more flexible and powerful. However, these strategies are inadequate for the increased flexibility and performance that ubiquitous computing environment requires because such systems can not utilize effectively all benefit from this environment. In this paper, we propose a solution based on risk to make use of many context parameters in order to provide good decisions for a safety environment. We design a new model for risk assessment in ubiquitous computing environment and use risk as a key component in decision-making process in our access control model.*

Keywords: context, risk, access control

1 Introduction

Ubiquitous computing integrates computation into 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, so they can not guarantee a good security in a distributed and dynamic environment like ubiquitous computing environment.

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 such highly dynamic and unpredictable as ubiquitous computing environment, we encountered several problems in making decisions. The previous context-based access control mechanisms almost use context based on decision tree. When we have so many context parameters, the decision tree is going to explode in space, leading to serious decrease in performance in both processing and management.

Our solution for this problem is using risk. Risk is the potential harm that may arise from some present processes or from some future events. It is often mapped to the probability of some events which is seen as undesirable. We have 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 [10].

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 with risk, we can make good decisions.

This paper provides an access control mechanism based on risk assessment and context. We use risk assessment to assist the decision-making process at access control manager. Both of them 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 a briefly review of a technique called multifactor evaluation process (MFEP) which is very important in our risk estimating process and a schema showing how to apply this method to calculate risk value and make decisions. Section 5 is our design of risk assessment mechanism, how it works with the context and other parameters. Section 6 presents a case study for our approach. Section 7 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 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] 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.

M. Strembeck and G. Neumann [14] also use context in their model. They introduce the notion of context constraint as certain context attributes must meet certain conditions to permit a specific operation.

These three above papers really make the access control dynamic and flexible but the decision-making process is not effective. They did not consider the aspect of security in making-decision process and the impact of security problems on the system. The solutions can not make use of many context parameters in the environment because they are not powerful enough.

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.

Our solution solves such problems by considering risk as an important factor in access control, using risk directly in making decisions. We utilize all information from environment, process them in a novel risk assessment model based on multi factor evaluation process. Moreover, we additionally include a new metric into this model which based on three important factors of security: availability, integrity and confidentiality. By doing this, we create a powerful, flexible access control model and improve preciseness in each access control decision.

3 Access Control Model with Risk Assessment

3.1 The Access Control Framework

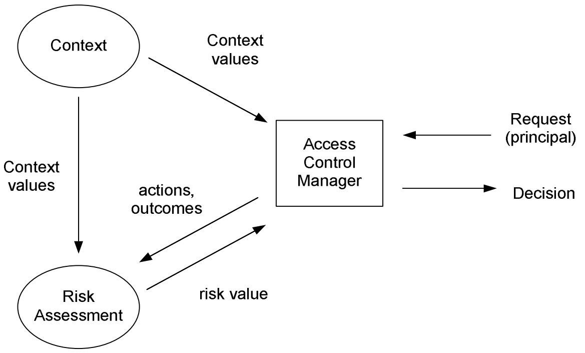

Figure 1. Access Control Framework

This section presents the framework of our access control system. There are three modules in the system as in figure 1. 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 ubiquitous middleware systems like CAMUS Server in [13].

3.2 Access Control Model

A request from principal p to perform an action is submitted to the access control manager. Access control manager looks up relevant outcomes that may occur due to this action and queries risk assessment module for calculating risk value after sending necessary parameters to it. The risk assessment module, after calculating cost of outcomes in term of availability, confidentiality, and integrity based on context of principal, environment and resource, evaluates risk value of the action. Decisions are 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.

Here we define some notions for this model.

Definition 3.1. A user, a process or a resource which interacts or can interact with other users, processes or resources is called a principal.

In this paper, we denote a principal by P.

Definition 3.2. Each principal can perform some allowed actions. A set of allowed actions that is available for principal P is called a set of action A.

We denote an action in a set of action by a.

Definition 3.3. An outcome (o) of an action is a consequence under all possible combinations of the action and states. A set of outcome (O) is a set of consequences of an action in a set of action A.

Definition 3.4. Context is information related to current action, consisting of information from principal, surrounding environment, and the system. For example, they can be time (night, daytime…), location (in-building, in-office, outside), network state, state of resource.

Definition 3.5. Consequence function, c(o), is a function for calculating cost of each outcome (o) in the specific state. These values are evaluated by loss of confidentiality, availability, and integrity.

Definition 3.6. Risk function RV(o,a) is a function for calculating risk value of the action in the current state. The system bases on this value to work out the decision.

4 MFEP and risk assessment schema

4.1 MFEP

In reality, we have many decision making problems that need to consider many factors. MFEP deals with these problems with a quantitative approach in cases where all of the important criteria can be given appropriate numerical weights and each alternative can be evaluated quantitatively in terms of these criteria [15].

MFEP consists of three steps:

- Step 1: List all factors and give to factor i a weight FW_i ($0 \leq FW_i \leq 1$)

- Step 2: Factor evaluation

With each factor I, we assess solution j by giving it a coefficient FE_{ij} (called evaluation of solution j under factor i)

- Step 3: Total weighted evaluation

$$TWE_j = \sum_i FW_i \times FE_{ij}$$

Considering these values TWE_j we can choose the best solution.

4.2 Risk assessment schema

Based on MFEP method, we propose a risk assessment schema in order to make decision for the system. The schema consists of five steps as followings.

- Step 1: Identify allowed actions in service, and outcomes of each action.

- Step 2: Assign weight for each factor availability, integrity, confidentiality to the service.

- Step 3: Specify cost of each outcome in term of availability, integrity, confidentiality for service.

- Step 4: Identify probability of outcomes (f), based on the set of current context and probability of them.

- Step 5: We have two solutions: “Accept” or “Reject”, and risk value of action in term of availability, integrity and confidentiality in both two solutions. Apply MFEP with the above parameters and choose the better solution.

Step 1, step 2 and step 3 of this schema must be performed by administrator and service provider at the first time the service is installed in the system. The rest is done automatically by risk assessment module whenever system needs to make decisions.

5 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 than when we use wired connection.

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

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

5.1 Risk of outcome

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

In aspect of principal 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 principal), $i \in N$

- $o_{a_i,j}$ is an outcome in set of outcome O of action a_i, $j \in N$

- $c_A(o_{a_i,j})$ is cost of outcome $o_{a_i,j}$ in term of availability

- $c_I(o_{a_i,j})$ is cost of outcome $o_{a_i,j}$ in term of integrity

- $c_C(o_{a_i,j})$ is cost of outcome $o_{a_i,j}$ in term of confidentiality

- s_k: is a state 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, risk value of the outcome in term of availability is:

$$RV_A(o_{a_i,j}) = c_A(o_{a_i,j}) \times \sum_k f_{o_{a_i,j},s_k} \qquad (1)$$

Risk value of the outcome in term of integrity is:

$$RV_I(o_{a_i,j}) = c_I(o_{a_i,j}) \times \sum_k f_{o_{a_i,j},s_k} \qquad (2)$$

Risk value of the outcome in term of confidentiality is:

$$RV_C(o_{a_i,j}) = c_C(o_{a_i,j}) \times \sum_k f_{o_{a_i,j},s_k} \qquad (3)$$

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

5.2 Risk of action

Risk value of an action is sum of risk value of all outcomes of the action. We can calculate risk value of each action in term of availability, integrity and confidentiality one after another.

For availability:

$$RV_A(a_i) = \sum_j RV_A(o_{a_i,j}) \quad (4)$$

For integrity:

$$RV_I(a_i) = \sum_j RV_I(o_{a_i,j}) \quad (5)$$

For confidentiality:

$$RV_C(a_i) = \sum_j RV_C(o_{a_i,j}) \quad (6)$$

in which $i, j \in N$.

5.3 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:

$$RV = \frac{w_1 RV_A + w_2 RV_I + w_3 RV_C}{w_1 + w_2 + w_3} \quad (7)$$

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.

6 A Case study – Access control management in a health care system

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. 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 can be viewing a record, modifying some information, upload data, etc.

Access control system will use contextual information to work out the decision of authorizing access to the record. For example, if user is the doctor and he is now in emergency room, he can do any actions he wants without considering the risk. But in the case the doctor requests the access to the record from a terminal outside the hospital, access control system will take into account the risk created by this context. Even if the doctor is in the hospital but not in emergency room, the system still needs to consider the context of time if it is in rush-hour or not in the working time and uses it to calculate risk value.

Beside location and time, in this scenario we need to consider network condition, size of data, current number of transactions and other context parameters.

Considering the action "viewing record", it has some outcomes such as unavailable, service-corrupted, leaking information, etc. 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.

Applying the risk assessment schema in section 4.2, we specify weight for 3 criteria of this service: availability, integrity and confidentiality. For example, we have the weight for each criterion as followings:

Table 1.

Factor	Factor weight
Availability	0.3
Integrity	0.4
Confidentiality	0.3

We have a metric system for evaluating cost of each outcome to each of three above criteria: availability, integrity and confidentiality. With: (0: no impact, 1-2: small impact, 3-5: medium impact, 6-8: big impact, 9-10: extreme impact).

Here we have two alternative solutions. One is "Accept" and the other is "Reject". With "Reject", the outcome is "service is not available" and probability for having this outcome is 1.

We can see all example value in table 2 for the action "View record".

Table 2. Outcomes, risk value of "View Record"

Outcomes	Risk context /Probability	Cost		
		Availability	Integrity	Confidentiality
Unavailable	- Record too big, in rush-hour / 0.3 - Transaction session is nearly full / 0.6	*5*	*0*	*0*
Leaking information	- Data unencrypted, remote working / 0.6 - Connection is not secured, remote working/ 0.5	*0*	*0*	*1*
Service corrupted	-Connection is lost / 0.7	*5*	*0*	*0*

Also we assume that current context consists of "record too big", "in rush-hour", "data unencrypted" and "remote working".

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

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.

Using formula (1), (2), (3), we can evaluate risk of outcome "Unavailable" in term of availability, integrity and confidentiality:

$$RV_A(\text{"}Unavailable\text{"}) = 5 \times 0.3 = 1.5$$

$$RV_I(\text{"}Unavailable\text{"}) = 0 \times 0.3 = 0$$

$$RV_C(\text{"}Unavailable\text{"}) = 0 \times 0.3 = 0$$

Similarly, we evaluate risk of two other outcomes of action "View record":

$$RV_A(\text{"}Leaking\ information\text{"}) = 0$$

$$RV_I(\text{"}Leaking\ information\text{"}) = 0$$

$$RV_C(\text{"}Leaking\ information\text{"}) = 1 \times 0.6 = 0.6$$

$$RV_A(\text{"}Service - corrupted\text{"}) = 0$$

$$RV_I(\text{"}Service - corrupted\text{"}) = 0$$

$$RV_C(\text{"}Service - corrupted\text{"}) = 0$$

Risk for loss of availability of this action:

$$RV_A = 1.5 + 0 + 0 = 1.5$$

Then risk for loss of integrity and confidentiality:

$$RV_I = 0$$

$$RV_C = 0.6$$

Finally, we can calculate the risk value of action "View record". Using (7), the final risk value is the mean value:

$$RV = \frac{0.3 \times 1.5 + 0.4 \times 0 + 0.3 \times 0.6}{0.3 + 0.4 + 0.3} = 0.63$$

This value is the risk value of solution "Accept". We need to compare this value with risk value of solution "Reject".

Because "Reject" solution only have one outcome "Service is not available" with probability 1 and cost of this outcome for availability, integrity, confidentiality is respectively assigned 5, 0, 0. We easily have risk value of this action for "Reject" solution:

$$RV = \frac{0.3 \times 5 + 0.4 \times 0 + 0.3 \times 0}{0.3 + 0.4 + 0.3} = 1.5$$

Compare two risk value of "Reject" and "Accept", we choose the "Accept" solution which has smaller risk and the decision for the action "View record" is "Accept".

7 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 dynamic in management and flexible in handling access control. It provides a precise way to make decisions 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 to use 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 sessions also need to be flexible in order to support best services for customers. And we think efficiency will be much improved if the system can automatically update cost of outcomes of actions and detailed information of current network state based on evidence gathered from context framework, maybe through some intrusion detection systems or network management systems.

8 Acknowledgement

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2006-(C1090-0602-0002))

9 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.

[14] M. Strembeck, G. Neumann, “An integrated approach to engineer and enforce context constraints in RBAC”, ACM Transactions on Information and System Security, 2004, 7 (3): 392-427

[15] Render, B. & Stair, R. M., Jr. (1994), Quantitative

Analysis for Management, USA: Prentice-Hall, Inc.