Risk Assessment and Access Control for Ubiquitous Environments

Nguyen Ngoc Diep*, Sungyoung Lee*, YoungKoo Lee*, HeeJo Lee**
*Dept. of Computer Engineering, Kyung Hee University
**Dept. of Computer Science and Engineering, Korea University
e-mail : nndiep@oslab.khu..ac.kr

Abstraction

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.

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][5].

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 process or from some future event. It is often mapped to the probability of some event 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. 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, improving preciseness in each access control decision.

2. 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.

2.1. 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:

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

Risk value of the outcome in term of integrity is:

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

Risk value of the outcome in term of confidentiality is:

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

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

2.2. 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:

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

For integrity:

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

For confidentiality:

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

in which $i, j \in N$.

2.3. Risk value evaluation

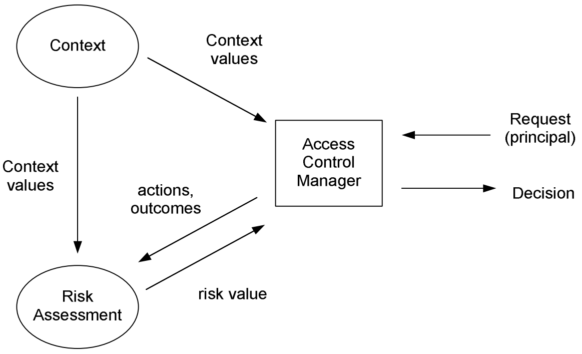
In fact, with each service, we consider the importance of each element different. For example, availability evaluation should be given more importance over the others in a case of downloading files.

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:

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

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

3. Access Control model with Risk Assessment



(Figure 1) Access Control Framework

There are three modules in the system as in figure 1. Access control manager 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 [6].

In reality, we have many decision making problems that need to consider many factors. Multi function evaluation process (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. Based on MFEP method [15], 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.

4. Conclusion

In this work, we have proposed 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.

In the proposed work, 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.

5. Acknowledgment

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITFSIP (IT Foreign Specialist Inviting Program) supervised by the IITA (Institute of Information Technology Advancement)

Reference

[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] 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.

[6] 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.

[7] 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

[8] Render, B. & Stair, R. M., Jr. (1994), Quantitative Analysis for Management, USA: Prentice-Hall, Inc.