Risk-aware Usage Decision Making in Highly Dynamic Systems

Leanid Krautsevich, Aliaksandr Lazouski
Department of Computer Science
University of Pisa
Largo B. Pontecorvo 3, Pisa, Italy
Email: krautsev@di.unipi.it
lazouski@di.unipi.it

Fabio Martinelli, Artsiom Yautsiukhin
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche
G. Moruzzi 1, Pisa, Italy
Email: fabio.martinelli@iit.cnr.it
artsiom.yautsiukhin@iit.cnr.it

***Abstract*—Usage control model (UCON) is based on the idea that attributes required for decision-making can be changed over a period of usage. Since it is not always possible to get a fresh and trustworthy value of attributes, a decision has to be done with some uncertainties in mind. Moreover, modern systems become more distributed and dynamic and this evolution aggravates the problem. Such trend demands for the solutions capable of working with imprecise values. Our study concerns analysis of risks to make access decision of usage control more credible. We consider the risks associated with imperfect mechanisms collecting information about an authorization context. To cope with these risks we introduce our approach based on Markov chains, which aims to help in making a decision to allow further access or to deny it. The proposed approach could be useful for designers of the policy enforcement engines based on the UCON model.**

***Keywords*-security; usage control; UCON; risk assessment; freshness of attributes; trustworthiness of attributes.**

I. Introduction

The main goal of any access control is to guarantee that a resource is used as it is stated in established policies and to prevent unauthorized users from accessing or corrupting the resource. A policy decision point entails the most complete, up-to-date and trustworthy information to make credible decisions. Obtaining such information is a difficult task since the mechanisms collecting authorization context are procedural, error-prone, rely on software and hardware, and, thus, have a risk of failure. Moreover, there is always a risk that the mechanisms are compromised by a malicious entity. Decisions made using low quality, vague, or obsolete information may result in major losses.

An authorization context received by a policy decision point can be imprecise because of two types of causes: unintentional and intentional ones. Unintentional causes appear because the system is imperfect and inherent risks are always present (e.g., delays, noise, loss of connection, etc.). Intentional causes are connected with deliberate alteration of authorization context by a malicious data provider. Note, that a malicious data provider may use unintentional causes to hide its actions.

All these drawbacks relevant for the access control model are even more relevant for its successor, the usage control model, where correctness of policies has to be checked not only during the first authorization, but also *afterwards*, i.e., during usage of a resource. We can check a policy only in discrete moments of time and there is no guarantee that the policy holds between adjacent checks. In highly dynamic systems this may lead to great losses. The reliability of controlling mechanisms is also limited by presence of design and implementation errors, vulnerabilities of execution environment, errors caused by users, etc. Thus, correct values of attributes may alter while the compromised controlling mechanisms do not detect this change.

In this paper we propose a basic risk-based approach which can helps in making decision for usage control model when a number of uncertainties are present. To the best of our knowledge, the risk-aware enforcement of usage control policy has not been addressed yet by the research community. The current state of the art gives some ideas about employing risk assessment for access control [1], [2], [3]. All these approaches focus only on an authorization decision which is made before granting access. In our work we stress the dynamic nature of UCON and consider how changes of authorization context may affect access decisions.

A. Main contributions

The main contributions of our study are the following:

1) We list uncertainties of different kinds and show how they affect the decision making process.
2) We provide a probabilistic approach based on Markov chains to model mutability of authorization context. The approach can be used to solve different problems caused by presence of uncertainties while here we stress only some of them.
3) We employ risk analysis in order to make the most rational decision and be as flexible as possible.

The rest of the paper is organized as follows. We start with a brief description of relevant aspects of UCON (Section II) and risk assessment (Section III). Then, we discuss possible risks which may cause uncertainties in received values of attributes (Section IV). Our basic approach is described in

This work was partly supported by the EU-FP7-ICT CONSEQUENCE project

Section V. Section VI provides some observations about the approach. Finally, we conclude the paper with related work (Section VII) and conclusions (Section VIII).

II. Usage control model

Usage control (UCON) proposed by Sandhu and Park [4] demands for persistent control over resources. Continuity of control is a specific feature of UCON intended to operate in an inconstant context. This inconstancy is a result of the entire usage process or caused by other uncontrollable factors. The context is formed by attributes of requesting a subject, an accessed object and execution environment.

A state of a UCON protection system is characterized by values of these attributes. The three system states are: "pre" (before access to the resource is granted and usage starts), "on" (access is granted and usage is ongoing) and "post" (usage is ended by a subject or terminated by a system). UCON security policies restrict subject's behavior and define which usages for the subject are permitted. UCON policy statements are built using *authorizations* (predicates over subject and object attributes), *conditions* (predicates over environmental attributes), and *obligations* (actions that must be performed along usage process).

Similar to [5], [6], we consider only authorizations in the paper since we are interested in evolution of attributes. Authorizations are assumed to consist of a set of attribute clauses, built of *one* attribute variable and a threshold, in a conjunctive normal form. The attribute clause (predicate) is a logical function mapping the attribute value to either true or false. An attribute clause may contain more attributes and have a more complex structure but we leave this complex issue for future work. For more details on UCON formal models we refer the reader to [7], [8].

III. Risk in usage control

Currently all decisions made in UCON are done assuming that input information is exactly as it is in reality. Although much can be done to assure that the information is valid it is practically impossible to eliminate all uncertainties at all. The more dynamic and distributed the Internet becomes the less certain we are in correct operation of a remote part of a system even if some controllable mechanisms are installed.

Although we cannot eliminate uncertainties from the real world we can adjust our perception of real-world situations. One way of doing this adjustment is to incorporate a notion of risk in decision making for UCON. Analyzing risk we can weight pros and cons of granting or revoking access.

Mathematically, risk is usually considered as follows [9]:

$$Risk = Probability\_of\_event \times Impact \tag{1}$$

In the context of UCON, a bad event occurs when access is granted with violation of some policy statements. Such violation may occur because of an unnoticed change of an attribute (i.e., uncertainty). We assume that in the beginning all values were correct (otherwise we should consider another problem).

An unnoticed change of an attribute leads to a direct loss only in some cases. First of all, change of an attribute may not violate the corresponding policy. For example, a student who just became 24 several months ago is still allowed for a discount for a bus tickets (he must be less than 26) even if his new age has not been inserted in a database. Sometimes violation of a policy is not a direct loss for the overall operation of a system, but we consider that an analyst already takes average loss for policy failure, i.e., implicitly multiplies the real loss of the system by a probability that violated policy leads to a failure in the system. The initial step in explicit analysis of the later relation can be found in [10].

IV. Intentional and unintentional risks

In this paper we consider the two types of uncertainty caused by unintentional and intentional changes.

A. Freshness of attribute values

Since the UCON model assumes that attributes may change, fresh values of the attributes are essential for a correct access decision [11], [5]. Thus, timely delivery of data is an important problem. Such problem has to be taken into account in highly dynamic systems where attributes change frequently but the value cannot be pushed to or pulled by a decision point so often. We consider the following types of this problems:

1) A fresh value can be obtained but the procedure costs some resources (e.g., bandwidth, power). In this case we need an efficient schedule for checking attribute changes.
2) It is practically impossible to get a fresh value when it is required. In this case we need to make a decision with some uncertainty which is still present.

These problems can be seen as particular cases of *timeliness* and *currency* factors from Bouzeghoub and Peralta [12]. Our first type relates to the problem of defining the frequency of updates (timeliness), while the second type is caused by a natural delay in delivery of the data (currency).

Example 1: We have a network of sensors and a central decision point (server). Sensors have limited resources (power, bandwidth, memory). Thus, the decision point receives fresh values of attributes only once in an hour. If a value exceeds a threshold of a policy statement during this hour the server will make an incorrect access decision.

Example 2: An on-line auction system allows sellers with good trustworthiness rating (above 1) to sell goods. The problem is that the trustworthiness rating is updated only after several weeks when the system receives feedback from a buyer. Thus, the decision to allow selling goods to a seller is based on a trustworthiness rating which is several weeks old. During this time a malicious seller may sell a great number of fake goods. This period cannot be reduced and the system has to be set up to make a decision with some uncertainty.

B. Correctness and trustworthiness of attributes

A resource provider often relies on remote sensors controlled by other entities to acquire the required attributes. Therefore, the received attributes can be only partially trusted. In order to increase the trustworthiness of the received values the collection of attributes may be enforced or monitored. Unfortunately, non of these ways is perfect: monitoring mechanism can be faked, enforcement can be broken. Therefore, even if some method of control is installed we still do not have 100% assurance that the received data is correct.

Example 3: In a hospital doctors can access patient's records. Junior doctors can access records of their own patients only, ordinary doctors - records of all patients from the corresponding department, senior doctors - all records. Mr. Johns who was employed by the hospital only 4 month ago as a junior doctor after next login to the system wants to access data of a patient from another department and shows credentials of a senior doctor. Though the situation can be ordinary (e.g., Mr. Johns got a quick promotion) it is very improbable, because the average time between promotions is 3 years. The system should weight the risk of granting and denying access to the suspicious doctor (which is, probably, trying to fool the system). Note, that the system denying access may simply ask a higher authority for confirmation in such suspicion requests (or allow the access, but notify the high authority).

V. Basic risk-aware approach for making decision under uncertainties

The proposed approach consists of the following steps:

1) For each attribute create a Markov chain for modeling changes of attribute values.
2) Compute the probability that the policy which uses the attribute is violated at some point of time.
3) Compare costs if further access is allowed or denied.
4) Apply a mitigation strategy to reduce the risk.

A. Markov Model for attributes

The first step is to create a Markov chain, which indicates how a value of an attribute changes. States in this chain are possible values of the considered attribute and transitions are possible changes of the attribute. States can be combined if a fine-grained analysis is not required for simplicity.

Example 4: A Markov model for the auction from Example 2 is depicted in Figure 1. For a particular seller we can assume that transition probabilities μ, η, and o are the same for all states. These parameters can be updated periodically to be up-to-date. The grey circles denote the states are where the policy is violated (bad states).

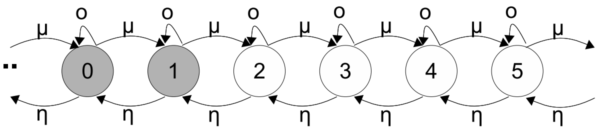

Figure 1. Markov model for Auction

In this paper we assume that transition probabilities do not change during some period of time (strict-sense stationary systems [14]). Moreover, the change of these probabilities occurs slowly and infrequently. This assumption allows us to observe these values in the past and use them for prediction of nearest future. This is an ordinary practice in many statistics-based prediction methods (e.g., risk assessment [9], [13]).

In practice, transition probabilities can be estimated using statistics about past operations. The best way is to find the statistics for a specific partner and derive the probabilities about it directly. This approach is useful if we consider a long term interaction with a partner. Another way is to get the value from other sources (e.g., other data providers) or a central authority (similar to credit bureaus in banking). Finally, if interactions with partners are very short (e.g., web server and users) then similar users can be grouped and statistics can be collected for the whole group.

B. Computation of probabilities

Now we compute the probability of failure of a policy. We need to know the amount of transitions in the period between the time when we know exact value of an attribute and the current time. In the simplest case we know the amount of completed transitions (e.g., the auction server knows the exact amount of accomplished deals). In a general case, we can use the Poisson distribution for determining the number of transitions. Let:

- A be a set of all names of attributes ($a \in A$);
- pol_i be the policy which uses attribute a_i.
- $p_i(t)$ be the probability that the policy pol_i fails before time t.
- X_i be a domain of values of attribute a_i ($x_i \in X_i$).
- t_0 be the time when exact value of an attribute is known
- t' be the time when we would like to know $p_i(t')$.
- n_{mean} be the average amount of transitions in a unit of time (found from statistics).
- $p_P(n)$ be the probability that during the interval $t' - t_0$ exactly n transitions occur.

Using the Poisson distribution we find:

$$p_P(n) = \frac{\lambda^n e^{-\lambda}}{n!} \quad \text{where } \lambda = (t' - t_0) * n_{mean} \tag{2}$$

Now we are able to compute the probability that the attribute has a value x_i after n transitions ($p_i(x_i, n, t)$).

There is a vector of such probabilities: $S_i(t) = p_i(x_1, n, t), p_i(x_2, n, t), ..., p_i(x_k, n, t)$. $p_i, (x, n, t)$ can be found using Markov model theory and Kolmogorov-Chapman's equation in particular. Assume that we know the initial value (x_l) of the attribute at t_0. Thus, only $p_i(x_l, n, t_0) = 1$ and others are 0, i.e., $S_i(t_0) = \{0, 0, ...1, ...0\}$. The value of the vector at time t' will be

$$S_i(t') = S_i^T(t_0) * Prob_{qj}^n \tag{3}$$

where $Prob_{qj}$ is a transition matrix composed by the probability of transition from state q (row) to state j (column). $Prob_{qj}^n$ shows that the matrix is in power n.

Since we are interested only if the value reached a state in which the policy is violated, we should convert such states in *absorbing* states. Absorbing states are such states from which there are no other transitions but to the same state. Moreover, we can leave only those states to which there are transitions from good states. In order to convert a bad state to an absorbing state in the corresponding row l the probability in the column with the same number should have value 1 ($Prob_{ll} = 1$) and others - 0 ($Prob_{lm} = 0$ for $l \neq m$).

Example 5: Suppose that at the auction a seller has trustworthiness rating equal to 3 at t_0 and a policy states that the rating cannot be less than 2. We know that there were only 2 deals from t_0 to t'. Suppose that $\mu = 0.3$, $\eta = 0.5$ and $o = 0.2$. States '0' and '1' are absorbing states. Thus, the equation will be the following:

$$S_i(t') = \begin{pmatrix} 0.0 \\ 0.0 \\ 0.0 \\ 1.0 \\ 0.0 \\ 0.0 \end{pmatrix}^T \times \begin{pmatrix} 1.0, 0.0, 0.0, 0.0, 0.0, 0.0 \\ 0.0, 1.0, 0.0, 0.0, 0.0, 0.0 \\ 0.0, 0.5, 0.2, 0.3, 0.0, 0.0 \\ 0.0, 0.0, 0.5, 0.2, 0.3, 0.0 \\ 0.0, 0.0, 0.0, 0.5, 0.2, 0.3 \\ 0.0, 0.0, 0.0, 0.0, 0.5, 0.2 \end{pmatrix}^2 \tag{4}$$

Note, that there are more than 6 possible values for trustworthiness rating but here we show only the meaningful part of the matrix. Therefore, the sum of probabilities in the last row is not equal to 1.

When the vector of states $S_i(t')$ is found we simply sum up the values which belong to bad states.

$$p_i(n, t') = \sum_{x_j \in B} S_i(t')[j] \tag{5}$$

where B is a set of all bad states.

In case we know exactly the number of transitions between t_0 and t', than $p_i(t') = p_i(n, t')$. If we use the Poisson distribution to compute the amount of transitions we have to sum up also the product of probabilities:

$$p_i(t') = \sum_{n=0}^{\infty} p_P(n) * p_i(n, t') \tag{6}$$

Table I
DECISION MATRIX WITH COSTS

	Satisfied policy $(1-p_i(t'))$	Failed policy $(p_i(t'))$
Continue access	C_i^{CS}	$-C_i^{CF}$
Revoke access	$-C_i^{RS}$	C_i^{RF}

For practical reasons one can use a limit for $p_P(n)$ to determine a reasonable number of considered transitions N, e.g., $p_P(N) > 0.001$.

The same mathematical model can be used for determining the probability that after some time the attribute reaches some specific value x_s (the probability to be in state x_s). For this purpose only state x_s should be absorbing. Moreover, instead of summing probability values for all bad states (Equation 5) we should simply assign the corresponding probability:

$$p_i(n, t') = S_i(t')[s] \tag{7}$$

If we want to know the probability that the attribute will have exactly the value x_s at time t' we should simply use the same algorithm but without absorbing states.

C. Decision-making

There are two possible decisions about a usage session: to continue or to revoke the session. The decision depends on the attributes received by a decision-point. There are four possible results:

- continue usage when it should be continued;
- continue usage when it should be revoked;
- revoke usage when it should be revoked;
- revoke usage when it should be continued.

Each result should be evaluated before a decision is made. The value of the decision is a combination of possible risks and benefits that are connected with a particular decision (see Table I). The positive cost values in the table represent gains when negative values are losses connected with incorrect decision.

Decision theory provides a number of well developed methods to make a decision under risk and uncertainty [15]. Decision making under risk means that we know exact probabilities of policy failure (Equation 6). We apply a simple probability-weighted utility theory for analysis of alternatives (using Equation 1). The idea behind the analysis is to compare the benefits of allowing access and revoking it (i.e., alternative decisions). If we know that the probability of failure of policy pol_i at time t' is $p_i(t')$ then the access should be allowed if:

$$\begin{aligned} (1 - p_i(t')) * C_i^{CS} - p_i(t') * C_i^{CF} > \\ p_i(t') * C_i^{RF} - (1 - p_i(t')) * C_i^{RS} \end{aligned} \tag{8}$$

The formula is general, but in particular cases some parts can be omitted. For example, if reputation of the resource provider is not affected much by correct or incorrect decision than in many cases $C_i^{RF} = C_i^{RS} = 0$ and the formula becomes much simpler.

It is very difficult to determine the cost values for every single policy. Moreover, only the ‘losses caused by allowing access to a malicious user’ are policy specific, because violation of different policies have different impact on the overall operation of the system. Other cost values depend on the *overall* decision (allow or revoke) rather than on a concrete policy.

For making the overall decision, i.e., taking into account the overall risk for all policies, we should combine the probabilities for concrete policies. Losses caused by a potential abuse should be computed separately and then summed up ($-\sum_{\forall i} p_i(t) * C_i^{CF}$). On the contrary, the losses caused by incorrectly revoked access require satisfaction of all policies (multiplication of probabilities), but the cost itself does not depend on a concrete policy (-$\prod_{\forall i}(1-(p_i(t)) * C^{RS}$). The same strategy holds for allowing access to a honest user ($\prod_{\forall i}(1-(p_i(t))) * C^{CS}$). For denying access to a dishonest user we should find at least one violated policy ($(1-\prod_{\forall i}(1-p_i(t))) * C^{RF}$). Thus the whole inequality will become as follows:

$$\prod_{\forall i}(1-(p_i(t))) * C^{CS} - \sum_{\forall i} p_i(t) * C_i^{CF} > (1-\prod_{\forall i}(1-p_i(t))) * C^{RF} - \prod_{\forall i}(1-(p_i(t)) * C^{RS} \quad (9)$$

This formula allows a more comprehensive analysis coupled with simplifying the computation by reducing the number of required cost values.

D. Risk Mitigation

The proposed approach can be used in various situations depending on the type of uncertainties under consideration. The core schema is left the same: knowing the value at some moment of time we check the risk some time after and make a decision depending on the computed risk level.

In case we consider freshness of attributes, which cannot be updated very often, the proposed approach can show when the next check of values must be done. The decision point should wait for the time when Equation 8 (or Equation 9) will be false and ask for fresh data. Thus, risk can be used to make the updates only when they are really needed. Such efficient schedule saves computational and communication resources, on the one hand, and prevents unnoticed failures of policies on the other one. When updates of the values in arbitrary moments of time are impossible other mitigation strategies can be applied. One possibility is to suspend usage unless a new value, confirming good intends of the user, is received.

Example 6: The auction does not allow a seller to sell goods if his trustworthiness rating is below 2. If a seller with a low trustworthiness rating starts selling large amount of goods soon the negative reputation will be possible and if the possible losses overweight the possible benefits then the seller has to be banned until a real value of the rating will be received.

If we do not trust the values we receive from a sensor, we can use the approach to predict that the latest value is really a genuine one. Here we need the probability that the value of the attribute is exactly the one we received from the sensor (see the discussion at the end of Section V-B). Computing risk values we can make a decision to believe in the given values or to revoke the access. Thus, risk lets us to be more flexible making the decision and provides us with a new way of controlling access to resources.

VI. Discussion

In this paper we have proposed a basic approach based on the Markov chains. This basic approach requires many parameters which are often difficult to find in practice. On the other hand, as we have shown with the example about an auction the overall approach can be significantly simplified in many cases. Therefore, even if the theoretical approach requires definition of a complete matrix of probabilities only few of them actually should be determined in practice. Moreover, the required probabilities are not very sensitive for a company and can be shared easily (in contrast to the probability of attacks used in the security risk assessment).

Even though we have acknowledged that defining probabilities is a hard task we still assume that in many cases, when there is enough statistical data, the probabilities and mean number of transitions for the Poisson distribution can be found. Considering impact we also have shown that that only one cost has to be determined (the cost of allowing access to a dishonest user) for each policy, when other three costs are unique for the overall decision.

In this work, we focus only on the problem of predicting attribute values and making a rational access decision. Therefore, we did not consider some features of UCON which can be relevant for our approach. For example, we left behind the effect of obligations and applying some risk mitigation strategy on our approach. In contrast to [5] we have not considered enforcement of protection mechanisms. We also acknowledge that evaluation of complexity of computations must be performed (e.g., multiplication of matrixes can be an expensive operation). We are going to address these issues in the future work.

VII. Related work

Although we are aware of only one paper proposed for UCON based on risk assessment, several approaches for access control exist.

Aziz et al. [2] assess policies considering different types of risk - operational, combinatorial and conflict of interest. The approach is focused on reconfiguration of policy in a way to reduce its risk and save its strength. Han et al. [16] describe the approach to pre-evaluate security of policy using risk before enforcement. We don't consider composing of policies and assume that they are created in a secure way. Instead we discuss peculiarities of collecting fresh attribute values and problems connected with this issue.

Several approaches [17], [3], [18] use risk assessment to analyze cost of possible outcomes of access and employ a cost-benefit analysis to make an access decision. These methods consider a static decision making process while we analyze dynamic behavior of a system.

Krautsevich et al. [10] propose the first approach, to our knowledge, that empowers UCON model with risk assessment. This paper describes an approach for selection of service providers (data consumer) in a service oriented architecture (SOA). Our current work is devoted to another problem: enforcement of policies by a service provider and making a rational decision about further access for users.

Few methods describe trustworthiness of policy arguments and update mechanisms. Skalka et al. [1] discussed an approach to evaluate credentials for distributed authorization with risk. Nauman et al. [5] determined trustworthiness of update mechanism analyzing and verifying its behavior. Next to paying attention to trustworthiness of attributes our approach is also focused on their freshness and also explicitly shows how to make a decision using risk assessment.

VIII. Conclusion and future work

We have proposed a basic risk-based approach for UCON which is used in a highly dynamic environment. We have indicated several uncertainties which can lead to losses for a resource provider. Although these uncertainties have different nature (intentional and unintentional ones) we can apply similar solutions to make a reliable decision. We have shown a general, theoretical approach for dealing with the uncertainties and indicated how this approach can be applied in some specific scenarios. Although the approach can be seen very complex at the first glance, it becomes much simpler when applied in concrete scenarios. We also tried to make the approach as practical as possible.

The idea proposed in the paper is just an initial step in applying risk in UCON. We used a simple approach where each predicate is based on one attribute which in its turn can have good values or bad ones. The next step is to consider a more complex (more real) policy and improve our approach. This improvement should not affect the decision-making process, but only identification of probability of a policy failure. An interesting problem is to use the approach for considering behavior of an attribute in an interval (in contrast to some moment of time as we do in this work). Finally, we are going to implement our framework to estimate the complexity of the proposed analysis.

References

[1] C. Skalka, X. S. Wang, and P. Chapin, "Risk management for distributed authorization," *J. Comp. Sec.*, vol. 15, no. 4, pp. 447–489, 2007.

[2] B. Aziz, S. N. Foley, J. Herbert, and G. Swart, "Reconfiguring role based access control policies using risk semantics," *J. High Speed Networks*, vol. 15, no. 3, pp. 261–273, 2006.

[3] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-K. Lee, and H. Lee, "Enforcing access control using risk assessment," in *Proc. of ECUMN-07*, 2007, pp. 419–424.

[4] R. S. Sandhu and J. Park, "Usage control: A vision for next generation access control," in *Proc. of MMM-ACNS-03*, 2003, pp. 17–31.

[5] M. Nauman, M. Alam, X. Zhang, and T. Ali, "Remote attestation of attribute updates and information flows in a ucon system," in *Proc. of Trust-09*, ser. LNCS, Springer-Verlag, 2009, vol. 5471, pp 63–80.

[6] X. Zhang, R. Sandhu, and F. Parisi-Presicce, "Safety analysis of usage control authorization models," in *Proc. of ASIACCS*, 2006, pp. 243–254.

[7] A. Lazouski, F. Martinelli, and P. Mori, "A survey of usage control in computer security," IIT-CNR, Tech. Rep. IIT TR-12/2008, December 2008.

[8] J. Park and R. Sandhu, "The $UCON_{ABC}$ usage control model," *TISSEC*, vol. 7, no. 1, pp. 128–174, 2004.

[9] C. J. Alberts and A. J. Dorofee, "Octave criteria, version 2.0," CMU/SEI-2001-TR-016, Tech. Rep., December 2001.

[10] L. Krautsevich, A. Lazouski, F. Martinelli, and A. Yautsiukhin, "Risk-based usage control for service oriented architecture," in *Proc. of PDP-10*, IEEE, 2010.

[11] A. Pretschner, M. Hilty, and D. Basin, "Distributed usage control," *ACM Comm.*, vol. 49, no. 9, pp. 39–44, 2006.

[12] M. Bouzeghoub and V. Peralta, "A framework for analysis of data freshness," in *Proc. of IQIS-04*, 2004, pp. 59–67.

[13] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," NIST, Tech. Rep. 800-30, 2001.

[14] O. C. Ibe, *Fundamentals of Applied Probability and Random Processes*, T. Singer, Ed. Elsevier Academic Press, 2005.

[15] S. O. Hansson, "Decision theory. a brief introduction," available via http://www.infra.kth.se/~soh/decisiontheory.pdf on 20/11/2009, 1994.

[16] Y. Han, Y. Hori, and K. Sakurai, "Security policy pre-evaluation towards risk analysis," in *Proc. of ISA-08*, IEEE, 2008, pp. 415–420.

[17] L. Zhang, A. Brodsky, and S. Jajodia, "Toward information sharing: Benefit and risk access control (BARAC)," in *Proc. of POLICY-06*, IEEE, 2006, pp. 45–53.

[18] Y. Li, H. Sun, Z. Chen, J. Ren, and H. Luo, "Using trust and risk in access control for grid environment," *Proc. of SecTech-08*, 2008, pp. 13–16.