Influence of Attribute Freshness on Decision Making in Usage Control *

Leanid Krautsevich[1], Aliaksandr Lazouski[1], Fabio Martinelli[2], and Artsiom Yautsiukhin[2]

[1] Department of Computer Science, University of Pisa, Pisa, Italy
{krautsev,lazouski}@di.unipi.it
[2] Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy
{fabio.martinelli,artsiom.yautsiukhin}@iit.cnr.it

Abstract. The usage control (UCON) model demands for continuous control over objects of a system. Access decisions are done several times within a usage session and are performed on the basis of mutable attributes. Values of attributes in modern highly-dynamic and distributed systems sometimes are not up-to-date, because attributes may be updated by several entities and reside outside the system domain. Thus, the access decisions about a usage session are made under uncertainties, while existing usage control approaches are based on the assumption that all attributes are up-to-date.
In this paper we propose an approach which helps to make a rational access decision even if some uncertainty presents. The proposed approach uses the continuous-time Markov chains (CTMC) in order to compute the probability of unnoticed changes of attributes and risk analysis for making a decision.

Keywords: usage control, freshness of attributes, risk, continuous-time Markov chains.

1 Introduction

The usage control (UCON) model, proposed by Sandhu and Park [20], is a successor of access control which unifies recent advances in access control in one solid model. Access decisions in UCON are based on the values of attributes, similar to the attribute-based access control model [25]. The main peculiarity of UCON is the assumption that some attributes may change after granting access to a subject [16]. Thus, the access decision has to be made not only before a session, but also during the session. These principles of UCON are known as mutability of attributes and continuity of control.

The model works well until we are sure that values of attributes we have are the real current values. In fact, in some cases values of attributes used for the access decision making are old. Such situation happens because these attributes

* This work was partly supported by EU-FP7-ICT CONSEQUENCE and EU-FP7-ICT NESSoS projects.

might be checked only in some discrete points of time. The real values of the attributes between these points of time are unknown. Natural solution can be to reduce the interval between these points, but this is often impossible because of the cost of the checks (in terms of additional resources, bandwidth, CPU cycles required for getting and processing new data, etc.). Sometimes it is simply impossible to get fresh values of attributes because of natural delays of delivery (e.g., rating of an on-line seller is several weeks old because buyers provide their feedback only after some time after a deal is accomplished). Thus, we have to make an access decision using old, not fresh values.

Krautsevich et al. [13] proposed an approach based on risk analysis which helps to predict when possible losses caused by an incorrect decision overcome possible benefits in the presence of uncertainty. The authors proposed to exploit the discrete-time Markov chains in order to estimate the probability of a violation of security policies. The discrete-time Markov chains are well suited when the number of changes of an attribute is known (e.g., in an on-line auction, a number of accomplished deals is known, even if not all feedbacks have been uploaded). The authors also considered a simple policy: policy consisted of rules that contained one attribute and a threshold. Note, that risk in such approach arises because of imperfect system (impossibility to get fresh values of attributes) rather than because of existing threats for a system, as risk is usually used in the security community [23, 9, 5, 22, 7, 19].

The main contribution of this paper is the approach which is more suitable for the attributes for which we do not know how many times the attributes have changed, but know the time elapsed since the last check (when the exact value was known). Moreover, the current approach is applicable to more complex policies composed of atomic rules that makes the analysis more practical. We have shown that policies can be analysed in two different ways depending on the cause of losses (losses caused by failure of an attribute or failure of the whole policy).

The rest of the paper is organised as follows. We provide basic information about UCON, risk, and considered uncertainties in Section 2. Section 3 describes the running example used in the paper. We present a method for risk-aware decision-making on the basis of CTMC in Section 4. Section 5 describes the risk-aware decision-making for complex policies of several attributes. Possible risk mitigation strategies are outlined in Section 6. We conclude the paper with the related work (Section 7) and the conclusion and future work (Section 8).

2 Background

2.1 UCON

The most important features of the UCON model in the context of our paper are mutability of attributes and continuity of control. Mutability of attributes means that attributes required for making an access decision can change during a usage session. Therefore, it is not enough to evaluate attributes once before

the access is granted, but continuous evaluation is also required when the usage session is active.

Next to usual authorisations the UCON model also checks for conditions and obligations. Authorisations are the logical predicates which depend on attributes of subject and object (location of the subject, size of the object, etc.). Other attributes (of the environment in general) which can affect access decisions are taken into account in conditions (e.g., amount of space left on the hard disk, time of the access, etc.). Obligations are the actions which must be fulfilled (e.g., a subject must sign an agreement before accessing a resource). In this work we concentrated on authorisations and conditions only.

2.2 Risk Analysis

Risk is a well-known instrument for assessment for making decisions when some uncertainties present. The idea is to assess possible losses and compare them with possible benefits. In most cases risk is used to judge if a system is secure enough or some additional controls should be installed. Uncertainties in this cases are expressed as average probability that a threat will occur. The following well-known formula is used for computation of risk [9, 23, 1]:

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

In our paper we consider uncertainties about the actual values of attributes which are required for making an access decision.

2.3 Uncertainties

There are two types of unintentional uncertainties which arise during collecting of attributes: timeliness and currency [4]. These uncertainties may lead to incorrect decisions, i.e., allow access when it should be forbidden or grant access to an unauthorised party. Timeliness means that we cannot check an attribute very frequently because of some reasons (e.g., it is simply impossible, or impractical, or too costly, etc.). An example of such attribute could be position of a person every half an hour. Sending such information every minute will consume too much power, bandwidth, and CPU cycles of a monitoring system. Currency is a problem of other kind: there is a natural delay in the delivery of a fresh value. After accomplishing a deal an on-line buyer waits for the delivery, tests a product, and only then submits its feedback. All this time other buyers see the old reputation value of the seller. In our approach we take these two uncertainties into account by predicting a real value of an attribute and checking if access policies are satisfied.

Our approach can be also applied to some intentional uncertainties, though the problem has to be stated a bit differently. Imagine, we have one trustworthy value at some point of time. When we get a new value we may have some doubts about its trustworthiness, i.e., we believe that there is a possibility that the value is fake. Then, our task is to check how trusted is the recently sent value.

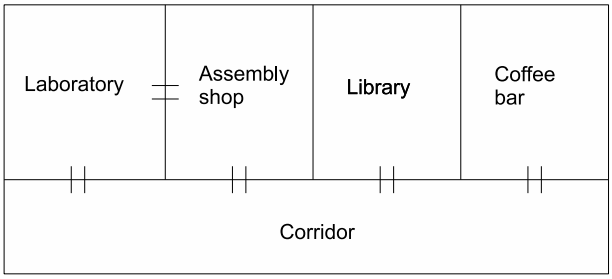

Fig. 1. Structure of the R&D department

3 Running Example

As a running example, we consider a research and development (R&D) department of a small company, which develops and produces prototypes of novel electronic devices. The department consists of a laboratory, an assembly shop, a library, a coffee bar, and the corridor, which connects all these rooms. There is an additional direct door from the laboratory to the shop. The structure of the company is presented in Figure 1.

In the example, we consider an engineer who works on a new project and uses a tablet computer for this purpose. In order to protect secrets about new devices from a possible leakage, the personnel is not allowed to access and use sensitive information outside of the laboratory and the assembly shop. The engineer is allowed to use his device outside of the laboratory and the assembly shop for any other purposes but for working on the project.

The position of any person which has access to trade secrets is controlled by a location tracking system. A special sensor is implanted into the tablet laptops which sends the information about the position of the device every 15 minutes. It has been found that often the engineers go to the coffee bar to take some coffee and do not close the usage session of projects. Thus, sometimes they have access to the secrete information outside of the allowed rooms, while sessions are still active and the next position check will be only several minutes afterwards. Reducing the period between position checks results in more power and bandwidth consumptions. Thus, there is a need for rational determination of the time when the check has to be scheduled.

4 Risk-aware Decision for Policy of One Attribute

In this section we consider the usage of an object that is controlled by a policy of one rule that constraints one attribute. The generalisation for policies of several rules is done in Section 5. We assume that we know a precise value of an attribute in some point of time in the past and would like to tell if we should continue the session or should stop it, even if there is some uncertainty about the current

value. In order to make a rational decision, we, first, compute the probability that the attribute has changed and its current value violates the policy. Then we apply risk management (using Formula 1) to make a decision under this uncertainty.

4.1 Computation of Probability

We start with the evaluation of the probability of policy violation. We consider a discrete attribute and assume that attribute satisfies the Markovian property, which means that a future attribute value depends only on the present value and does not depend on its previous values. Another assumption is that the average time between changes of attribute value exponentially distributed with the rate parameter v. These assumptions allow modelling the behaviour of attribute values using a CTMC.

The Markov chain contains states and transitions between states. The states of the chain represent the values of the attribute, and the transitions describe the changes of the attribute. The values of attribute can be grouped into two domains: the "bad" domain B and the "good" domain G. If the attribute takes a value from the "bad" domain then the policy is violated and the usage session should be revoked. If the attribute takes a value from the "good" domain then the policy holds and the usage is continued. The states of Markov chain can be gathered into two groups I_B and I_G respectively. The set of all values of attribute is $X = B \cup G$ and the appropriate set of states is $I = I_B \cup I_G$. In addition, we define the following variables:

- $x \in X$ is a value of the attribute. By x_i we denote the value of the state i;
- v_i is the rate parameter of exponential distribution for the time of jumping from state i to another state, the value $\frac{1}{v_i}$ is the average life-time of the attribute with the value x_i;
- p_{ij} is the one-step transition probability (the probability that the process makes a direct jump from the state i to j without visiting any intermediate state);
- t_0 is the time when we know the exact value of the attribute;
- t' is the time, when we make an access decision about the usage session. The last update of the attribute was at t_0.

We assume that the values v_i and p_{ij} can be determined and adjusted using statistical methods during the analysis of the past behaviour of the system. The history of an attribute changes between possible states is require for this purpose. Using v_i and p_{ij} we can evaluate the probability of policy violation on the basis of the approach described below.

The transitions between the states are described with the infinitesimal transition rates ($q_{ij} \in Q$). The infinitesimal transition rates are defined as

$$q_{ij} = v_i p_{ij}, \ \forall i, j \in I \text{ and } i \neq j. \tag{2}$$

The infinitesimal transition rates uniquely determine the rates v_i and one-step transition probabilities p_{ij}:

$$v_i = \sum_{\forall j \neq i} q_{ij}. \tag{3}$$

$$p_{ij} = \frac{q_{ij}}{v_i}. \tag{4}$$

Suppose, the value of an attribute is $x_i \in G$ (we are in state $i \in I_G$) at time t_0. We need to find the probability of $x_j \in B$ ($j \in I_B$) during the period from t_0 till t'. This problem is solved by replacing "bad" states with an absorbing state. An absorbing state is the state which the process can not leave. The way to model an absorbing state is to set leaving rates to zero. In our case the whole subset of states I_B should be replaced with one adsorbing state a. The modified Markov chain can be seen as

$$I^* = (I_G) \cup \{a\} \text{ and } v_i^* = \begin{cases} v_i, \forall i \in I_G; \\ 0, \ i = a. \end{cases} \tag{5}$$

The modified infinitesimal transition rates correspondingly:

$$q_{ij}^* = \begin{cases} q_{ij}, & \forall i, j \in I_G \text{ with } i \neq j; \\ \sum\limits_{k \in I_B} q_{ik}, & \forall i \in I_G, \ j = a; \\ 0, & i = a, \ \forall j \in I_G. \end{cases} \tag{6}$$

In the sequel, all indicators with $*$ refer to the Markov chain with absorbing states (e.g., q_{ij}^*, v_i^*, etc).

Example 1. The location attribute in the R&D department is a Markov chain of five states (see Figure 2a). However, the number of states can be modified, because the access to the database should be forbidden if the researcher is in the library, the coffee bar, or the corridor. Thus, these states could be replaced with one absorbing state a. The modified Markov chain is presented in Figure 2b. The following one-step transition probabilities (P) and rates (V) have been determined according to the past observations.

$$P = \begin{bmatrix} 0 & 0.7186 & 0 & 0 & 0.2814 \\ 0.7200 & 0 & 0 & 0 & 0.2800 \\ 0 & 0 & 0 & 0 & 1.0000 \\ 0 & 0 & 0 & 0 & 1.0000 \\ 0.4976 & 0.4976 & 0.0021 & 0.0028 & 0 \end{bmatrix}, \quad V = \begin{bmatrix} 0.0167 \\ 0.0250 \\ 0.0083 \\ 0.0333 \\ 2.0098 \end{bmatrix}. \tag{7}$$

In the example we consider that time is measured in minutes. So the rate $v_1 = 0.0167$ means that the chain leaves state 1 with the average time $t_{avg} = \frac{1}{v_1} = 60$ minutes.

Let the matrix Q of the infinitesimal transition rates q_{ij} for initial chain be computed using Equation 2.

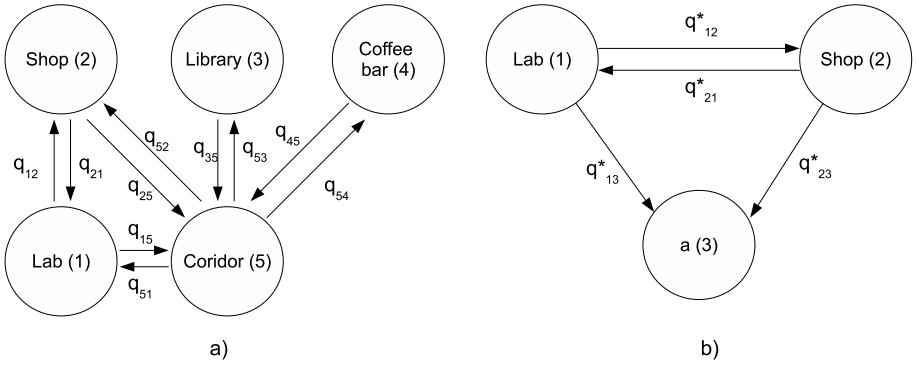

Fig. 2. Markov chains for User Location

$$Q = \begin{bmatrix} 0 & 0.0120 & 0 & 0 & 0.0047 \\ 0.0180 & 0 & 0 & 0 & 0.0070 \\ 0 & 0 & 0 & 0 & 0.0083 \\ 0 & 0 & 0 & 0 & 0.0333 \\ 1.0 & 1.0 & 0.0042 & 0.0056 & 0 \end{bmatrix}. \tag{8}$$

The matrix Q^* of the modified infinitesimal transition rates after inserting of the absorbing state according to Formula 6 is given by:

$$Q^* = \begin{bmatrix} 0 & 0.0120 & 0.0047 \\ 0.0180 & 0 & 0.0070 \\ 0 & 0 & 0 \end{bmatrix}. \tag{9}$$

The matrix V^* of the modified according to Formula 3 rates given by:

$$V^* = \begin{bmatrix} 0.0167 \\ 0.0250 \\ 0 \end{bmatrix}. \tag{10}$$

Now we need to find transient probabilities from the initial state i into absorbing state a , i.e., the probaility of policy violation. We apply the uniformisation method to compute transient state probabilities p^*_{ij} [12, 24]. The uniformisation method replaces a CTMC by a discrete-time analogue, which is more suitable for numerical computations. The uniformisation is done by replacing the transition rates of Markov chain v^*_i with a sole transition rate v^* such as

$$v^* \geq v^*_i, \ \forall i \in I. \tag{11}$$

Usually, the following strategy is applied:

$$v^* = \max_{\forall v^*_i \in V^*} v^*_i. \tag{12}$$

The discrete-time Markov chain makes a transition from a state with probabilities

$$\overline{p^*}_{ij} = \begin{cases} \frac{v_i^*}{v^*} p_{ij}^* = \frac{q_{ij}^*}{v^*}, \ \forall\, i \neq j; \\ 1 - \frac{v_i^*}{v^*}, \qquad\qquad \forall i = j. \end{cases} \tag{13}$$

Now we have all required parameters and we can skip the mathematical proofs, which can be found here [24, pages 167-168]. Finally, the transition state probabilities can be found as

$$p_{ij}^*(t') = \sum_{n=0}^{\infty} e^{-v^*(t'-t_0)} \frac{(v^*(t'-t_0))^n}{n!} \overline{p^*}_{ij}^{(n)}, \ \forall i, j \in I \text{ and } t' > t_0. \tag{14}$$

where $\overline{p^*}_{ij}^{(n)}$ can be recursively computed from

$$\overline{p^*}_{ij}^{(n)} = \sum_{x_k \in I} \overline{p^*}_{ik}^{(n-1)} \overline{p^*}_{kj}, \ n = 1, 2... \tag{15}$$

starting with $\overline{p^*}_{ii}^{(0)} = 1$ and $\overline{p^*}_{ij}^{(0)} = 0$ for $i \neq j$.

For fixed $t' > t_0$ the infinite series can be truncated because of the negligible impact of the residue. The truncation number M (upper limit of summation) in Formula 14 can be chosen as

$$M = v^* t' + c\sqrt{v^* t'} \tag{16}$$

for some c with $0 < c \leq c_0(\varepsilon)$, where ε is a tolerance number [24, page 169].

Equation 14 gives a matrix of probabilities. The probability of policy violation is $p_v = p_{ia}^*(t')$ in case we consider the transition from the state i to the absorbing state a.

Example 2. We continue Example 1. Choose $v_{max}^* = \max_{V^*} v_i^* = 0.025$ according to Formulas 12 and 10. The matrix $\overline{P^*}$ of transition probabilities for the discrete-time Markov chain according to Formula 13 is given by:

$$\overline{P^*} = \begin{bmatrix} 0.33 & 0.48 & 0.19 \\ 0.72 & 0 & 0.28 \\ 0 & 0 & 1 \end{bmatrix}. \tag{17}$$

Suppose that we know that an engineer is in the lab (state 1) at time $t_0 = 0$. Using Formulas 14 and 15 we find that at $t_1' = 7$ minutes the probability that the engineer has left allowed area is $p_v^1 = p_{13} = 0.0330$, while the same probability after $t_2' = 14$ minutes is $p_v^2 = p_{13} = 0.0659$.

	Satisfied policy	Failed policy
Continue access	C^{CS}	C^{CF}
Revoke access	C^{RS}	C^{RF}

Table 1. Decision matrix

4.2 Decision Making

Two possible decisions about the further access are to continue or to revoke the access. Therefore, possible outcomes of such decisions under uncertainty are:

- usage session is continued when it should be continued;
- usage session is continued when it should be revoked;
- usage session is revoked when it should be continued;
- usage session is revoked when it should be revoked.

Every outcome either results in some benefits or losses. Therefore, we assign a cost to every outcome (see Table 1). The cost is a qualitative value (e.g., the amount of money) which represents the utility of the outcome for the company. We assume that the cost is positive if the right decision is made (e.g., the resource owner gains benefits allowing usage for a unauthorised subject). The cost is negative in the case of wrong decisions (e.g., the resource owner suffers losses if the access is granted erroneously).

Usually, the benefit of allowing the access to a right user is a fixed value, e.g., a user pays money for the usage of a resource to the resource provider. The benefit of revocation of the access to a malicious user often is zero, because there is no explicit benefit of such action. The loss of allowing access to a malicious user is either policy specific or depends on the nature of the attributes (see Section 5.2). The loss of revoking access of a regular user is, usually, results in some loss of reputation, however sometimes losses caused by revoking access to a regular user are significant since in this case we also have loss of productivity.

There is a well developed decision theory [11] that allows making a decision under risk and uncertainty. We apply the probability-weighted utility theory for analysis of alternatives. The idea is to compare risks of allowing access and risk of denying access.

We know the probability of policy violation $p_v(t')$ at the moment of time t' which has been found in Section 4.1. According to the Formula 1 the possible benefit of allowing further access is $(1-p_v(t'))*C^{CS}$. On the other hand, allowing access we also suffer some losses: $p_v(t') * C^{CF}$. The same logic can be applied to another alternative (to revoke access). Thus, the access should be allowed if:

$$(1 - p_v(t')) * C^{CS} - p_v(t') * C^{CF} > p_v(t') * C^{RF} - (1 - p_v(t')) * C^{RS} \quad (18)$$

Example 3. The example of the decision matrix is presented in Table 2. Suppose the company gains $C^{CS} = 20$ Euro in average per one access of a trusted user to the database, and the access of a malicious user results in losses C^{CF} of 2000

	Satisfied policy	Failed policy
Continue access	20	-2000
Revoke access	-100	0

Table 2. Example of the decision matrix

Euro. If the work on the project is idle because the access of the trusted user is revoked the company loses 100 Euro (C^{RS}). If the malicious user is prevented of accessing the database the company gains no benefits and suffers no losses ($C^{RF} = 0$).

The probability of policy violation after $t'_1 = 7$ minutes is $p_v^1 = 0.0330$. When we apply Formula 18 we see that $-46.6 > -96.7$, and the usage session can be continued. When we consider this inequality after $t'_2 = 14$ minutes ($p_v^2 = 0.0659$) we see the opposite situation: $-113 < -93.4$, and the usage session should be revoked or some mitigation strategy should be applied.

The start of a process from different states can lead to different decisions about the usage session. The probability of policy violation after $t'_3 = 10$ minutes is $p_v^3 = 0.0471$ if the process start from the state 1 (the engineer is in the laboratory), in this case $-75.1 > -95.3$ and the access can be continued. The probability of policy violation after $t'_3 = 10$ minutes is $p_v^3 = 0.0658$ if the process starts from the state 2 (the engineer is in the assembly shop), in this case $-113 < -93.4$ and some mitigation strategies should be applied.

5 Risk of Violation of Complex Policy

Frequently, a policy consists of a number of complex usage rules. A complex rule contains several atomic rules, that constrain different attributes of a subject, an object, and an environment. In our paper we consider only the following three operators for aggregation of rules: conjunction (AND), disjunction (OR), and negation (NOT). These are basic operators, though the approach can be extended for specific operators if needed (e.g., using the operations from [3]).

We assume that the attributes are statistically independent. This property can be guaranteed by the policy designer that should choose attributes in a proper way. In case when dependent rules (i.e., rules which are constructed using the same attributes) appear in the same complex policy conditional probabilities have to be used (i.e., probability of failure of one rule with the condition that another rule fails).

5.1 Combination of Probabilities

The probability that a complex rule does not hold can be assessed using the probabilities that atomic rules do not hold. An atomic rule r constrains one attribute and the probability p_r of rule violation is assessed using CTMC or any other method. Consider two simple rules α and β with probabilities of violation

p_α and p_β. The probability of violation p_γ of the complex rule γ is computed as follows:

$\gamma = \alpha\ AND\ \beta$ **:** the rule γ fails in three cases: when the rule α fails and the rule β holds, when the rule β fails and the rule α holds, or when they both fail simultaneously. Therefore, the probability of the failure of the complex rule γ is a summation on the probabilities of each case.

$$\begin{aligned} p_\gamma &= p_\alpha \oplus p_\beta \\ &= p_\alpha * (1 - p_\beta) + (1 - p_\alpha) * p_\beta + p_\alpha * p_\beta \\ &= p_\alpha + p_\beta - p_\alpha * p_\beta \end{aligned} \tag{19}$$

$\gamma = \alpha\ OR\ \beta$ **:** the rule γ fails only if both rules α and β fail. Thus, the probability of failure of the complex rule γ is a multiplication of probabilities of failure of the rule α and the rule β.

$$p_\gamma = p_\alpha \otimes p_\beta = p_\alpha * p_\beta \tag{20}$$

$\gamma = NOT\ \alpha$ **:** the rule γ holds, when the rule α fails. Thus,

$$p_\gamma = \neg p_\alpha = 1 - p_\alpha \tag{21}$$

Example 4. Consider the following situation. An engineer involved in one project requires access to the data of another on-going project. A complex policy allows to do this only if the engineer is in the laboratory and either the manager of another project or the engineer's supervisor is in the laboratory as well. The simple rules are

- α is "the engineer is in the lab";
- β_1 is "the manager of the another project is in the lab";
- β_2 is "the engineer's supervisor is in the lab".

The complex rule γ can be seen as $\gamma = \alpha\ AND\ (\beta_1\ OR\ \beta_2)$. The probability of violation of the complex rule is p_γ.

$$\begin{aligned} p_\gamma &= p_\alpha \oplus (p_{\beta_1} \otimes p_{\beta_2}) \\ &= p_\alpha \oplus (p_{\beta_1} * p_{\beta_2}) \\ &= p_\alpha + p_{\beta_1} * p_{\beta_2} - p_\alpha * p_{\beta_1} * p_{\beta_2} \end{aligned} \tag{22}$$

5.2 Combination of Losses and Benefits

There are two possibilities for assigning costs to a complex rule. The first one is when four costs for the decision matrix (see Table 4.2) are assigned for the whole complex policy. This situation is applicable if the costs do not depend on the cause of policy failure. Thus, it does not matter which atomic rule fails, because

we suffer the same amount of losses. This situation is easy for policy-makers, because only 4 costs are required for computations. The risk-aware decision about a usage session for the complex rule is done in the same way as for a policy of an atomic rule. The only difference is that probabilities have to be computed using the formulas given in Section 5.1.

The second possibility is applicable when a more fine-grained analysis is required. In such case we need to distinguish between losses caused by a failure of one attribute or another one. Such situation usually happens when satisfaction of one rule is much more important for us than the satisfaction of another one. C^{CS} is assigned to the whole policy because we get this benefit only if all rules are satisfied. It also does not matter why access to a honest user has been revoked. Therefore, this loss (C^{RF}) is also rule-independent and should be assigned to the whole policy. We also assume that there is no difference why we revoked access of unauthorised person (C^{RS}).

The rule-dependent cost is the cost of a violation when the access has not been prevented (but is had to be). If one rule is more important than another one, we have to consider different losses (C^{CF}) caused by violation of corresponding rules. Thus, we should combine risks to tackle this issue.

$\gamma = \alpha \ AND \ \beta:$ The risk of failure of the complex rule γ in case of conjunction is a summation of risks. Here we follow the same strategy which is applied in usual risk assessment methodologies (e.g., [23, 1]) when there are several independent risks which should be considered together.

$$R_{\gamma}^{CF} = C_{\alpha}^{CF} * p_{\alpha} + C_{\beta}^{CF} * p_{\beta}. \tag{23}$$

When we combine other complex rules we do not already have separate costs. On the other hand here we simply should sum up all (n) risks:

$$R_{complex}^{CF} = \sum_{i=1}^{n} R_{i}^{CF}. \tag{24}$$

$\gamma = \alpha \ OR \ \beta:$ The risk of failure of the complex rule γ in case of disjunction is equal to summed up losses when all atomic rules fail. The idea behind this combination is the following. We suffer losses only when all rules fail, but in this case we suffer losses from failure of all rules.

$$R_{\gamma}^{CF} = (C_{\alpha}^{CF} + C_{\beta}^{CF}) * p_{\alpha} * p_{\beta}. \tag{25}$$

Combination of risks of complex rules if we have n or-brunches is

$$\begin{aligned} R_{complex}^{CF} = (\sum_{i=1}^{n} C_{i}^{CF})(\prod_{j=1}^{n} p_j) = (C_{1}^{CF} * p_1) \prod_{j=2}^{n} p_j + \dots \\ + (C_{n}^{CF} * p_n) \prod_{j=1}^{n-1} p_j = R_{1}^{CF} \prod_{j=2}^{n} p_j + \dots + R_{n}^{CF} \prod_{j=1}^{n-1} p_j \end{aligned} \tag{26}$$

$\gamma = NOT\ \alpha$: Negation influence only probability and, therefore, should be eliminated before considering losses. We propose to use Morgan laws in order to leave negations only for atomic rules where they can be easily used for changing probabilities as it is shown in Section 5.1.

Example 5. Consider the same example we had in Example 4, but let now the costs of violation be different. As it has been explained above, the following costs are assigned for the whole complex policy: C_{γ}^{CS}, C_{γ}^{RF}, C_{γ}^{RS}. Costs of failure of each atomic rule are: C_{α}^{CF}, $C_{\beta 1}^{CF}$, $C_{\beta 1}^{CF}$. The possible losses (R_{γ}^{CF}) caused by granting an access when, in fact, some rule has failed are:

$$\begin{aligned} R_{\gamma}^{CF} &= R_{\alpha}^{CF} + R_{\beta}^{CF} * p_{\beta 2} + R_{\beta 2}^{CF} * p_{\beta 1} \\ &= C_{\alpha}^{CF} * p_{\alpha} + C_{\beta}^{CF} * p_{\beta 1} * p_{\beta 2} + C_{\beta 2}^{CF} * p_{\beta 1} * p_{\beta 2} \end{aligned} \tag{27}$$

6 Possible Mitigation Strategies

In this section we discuss what to do when the condition of Equation 18 fails. Naturally, the simplest solution which comes to the mind is to revoke the further access. However, this simplest solution is not applicable in all situations and, often, by far not the best one. Note, that we make a decision based on probabilities and this means that we can be wrong.

Other mitigation strategies are possible. First of all, the current session can be simply suspended unless a fresh value is received and a solid decision can be made. Another possibility is simply to ask for a fresh value right in the moment when Equation 18 fails. This is, probably, is the best strategy in our running example. When none of the proposed strategies are applicable an additional attribute may be requested, which somehow mitigates a possibility of granting the access to an unauthorised subject. One more strategy is to rise an alarm which notifies a responsible person that a suspicious operation has taken place. This could be a message to an administrator or a marked event in a log file.

As you see an immediate revocation of an access is not the only possibility which can be followed by noticing a suspicious usage session. These strategies should help administrators to react appropriately depending on the environment where our risk-based decision making approach is applied.

7 Related Work

Risk has been used by several researchers for empowering access control. In all these papers risk is used to make an access decision taking into account that granting the access is connected with some threat. This source of risk is different from the one we use in our paper (uncertainties associated with a current value of an attribute).

Some authors use risk as a static parameter which simply helps to assign correct privileges taking into account possible losses [15, 10, 21]. For example,

Skalka et al. [21] discussed an approach for risk evaluation of authorisations, the formal approach is used to assess and combine the risks of assertions that is used in authorisation decision. Other authors use risk as a dynamically changing value which depends on the current value of possible losses and benefits as well as on the probability of abusing granting privileges by a concrete subject [26, 7, 17, 6]. Deip et al. [7] show how risk of granting access can be computed and a decision is made if risk is less than a threshold. McGraw [17] pointed out that risk should be compared with operational needs. Unfortunately, the author did not provide any information about how this risk and operational needs can be calculated. Zhang et al. [26] also did not show how risk is computed but stated that risk should be compared with possible benefits. The authors paid more attention to propagation of risk and benefits through a trust chain. Ni et al. [19] consider the parameters required for computation of risk as static, but use a notion of "access quota", which is given to a subject and reduces with access of subjects to some resources according to a risk level.

Several authors paid more attention to incorporating risk semantics in access policies rather than to the computation of risk. For example, the policy language, proposed by Aziz et al. [2], contains three types of risks: operational, combinatorial, and conflict of interest. Dimmock et al. [8] show how OASIS access control system and its role-based policy language can be extended with trust and risk analysis.

Krautsevich et al. [14] also applied risk analysis for usage control model in order to select the less risky data processor in service-oriented architecture. The authors also indicated how risk can change after granting access to a data processor and how the data processor can reduce its risk level to provide a better service.

Trustworthiness of policy arguments and update mechanisms have been also investigated by several authors. Nauman et al. [18] provide a way to verify the attribute update behaviour (together with information flow behaviour) and showed how this behaviour can be measured and analysed against UCON policies.

8 Conclusion and Future Work

In this paper we presented an approach which helps to make decisions even if values of attributes are not up-to-date. In this approach we do not need to know the amount of changes of attributes, but just time passes after the last update. Mutability of attributes was modelled by means of CTMC where states are possible attribute values, and transitions are possible changes of the attribute. This improvement makes the approach more realistic. We also considered more complex policies and determined how risk should be computed in such settings. We discovered that the cost of violation sometime depends on the attribute which can take an unwanted value or on the violation of the policy itself. In both cases aggregation of losses must be done differently. We suppose that in most cases the simplest analysis (e.g., when costs assigned to the whole policy) is applied and only in very specific situations the fine-grained analysis is required.

As the future work we would like to make the approach more effective by using the values (probabilities) found during the previous access check rather than recomputing the values from the beginning. Such on-line approach should significantly reduce computational cost. Another possible direction of the model improvement is to consider cases of dependent attributes. This issue requires complex mathematical models for implementing correlated Markov chains. In addition, we are going to elaborate the model for applying mitigation strategy and incorporate it in the overall framework more formally. Finally, we are going to make a prototype of the proposed usage control model in order to estimate possible overhead in the decision making process.

Acknowledgments. We would like to thank the anonymous reviewers for their helpful comments.

References

1. C. J. Alberts and A. J. Dorofee. OCTAVE Criteria. Technical Report CMU/SEI-2001-TR-016, CERT, December 2001.
2. A. B. Aziz, A. S. Foley, A. J. Herbert, and A. G. Swart. Reconfiguring role based access control policies using risk semantics. *Journal of High Speed Networks*, 15(3):261–273, 2006.
3. P. Bonatti, S. De Capitani di Vimercati, and P. Samarati. An algebra for composing access control policies. *ACM Transactions on Information and System Security*, 5(1):1–35, 2002.
4. M. Bouzeghoub and V. Peralta. A framework for analysis of data freshness. In *Proceedings of the International Workshop on Information Quality in Information Systems*, pages 59–67, 2004.
5. S. A. Butler. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering (ICSE'02)*, pages 232–240. ACM Press, 2002.
6. P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 222–230, Washington, DC, USA, 2007. IEEE Computer Society.
7. N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-K. Lee, and H. Lee. Enforcing access control using risk assessment. In *Proceedings of the Fourth European Conference on Universal Multiservice Networks (ECUMN'07)*, pages 419–424, Washington, DC, USA, 2007. IEEE Computer Society.
8. N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, and K. Moody. Using trust and risk in role-based access control policies. In *Proceedings of the 9th ACM Symposium on Access Control Models and Technologies*, pages 156–162, New York, NY, USA, 2004. ACM.
9. L. A. Gordon and M. P. Loeb. *Managing Cybersecurity Resources: a Cost-Benefit Analysis*. McGraw Hill, 2006.
10. Y. Han, Y. Hori, and K. Sakurai. Security policy pre-evaluation towards risk analysis. In *Proceedings of the 2008 International Conference on Information Security and Assurance (ISA'2008)*, pages 415–420, Washington, DC, USA, 2008. IEEE Computer Society.
11. S. O. Hanson. Decision theory: A brief introduction, August 1994.

12. O. C. Ibe. *Markov processes for stochastic modeling*. Academic Press, 2009.
13. L. Krautsevich, A. Lazouski, F. Martinelli, and A. Yautsiukhin. Risk-aware usage decision making in highly dynamic systems. In *Proceedings of the The Fifth International Conference on Internet Monitoring and Protection*, Barcelona, Spain, May 2010.
14. L. Krautsevich, A. Lazouski, F. Martinelli, and A. Yautsiukhin. Risk-based usage control for service oriented architecture. In *Proceedings of the 18th Euromicro Conference on Parallel, Distributed and Network-Based Processing*. IEEE Computer Society Press, 2010.
15. Y. Li, H. Sun, Z. Chen, J. Ren, and H. Luo. Using trust and risk in access control for grid environment. In *Proceedings of the 2008 International Conference on Security Technology*, pages 13–16, Washington, DC, USA, 2008. IEEE Computer Society.
16. F. Martinelli, P. Mori, and A. Vaccarelli. Towards continuous usage control on grid computational services. In *Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services (ICAS/ICNS '05)*, 2005.
17. R. W. McGraw. Risk-adaptable access control (radac). available via `http://csrc.nist.gov/news_events/privilege-management-workshop/radac-Paper0001.pdf` on 16/08/09.
18. M. Nauman, M. Alam, X. Zhang, and T. Ali. Remote attestation of attribute updates and information flows in a ucon system. In *Proceedings of the Second International Conference on Trust Computing.*, volume 5471 of *Lecture Notes in Computer Science*, pages 63–80. Springer-Verlag, 2009.
19. Q. Ni, E. Bertino, and J. Lobo. Risk-based access control systems built on fuzzy inferences. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pages 250–260, New York, NY, USA, 2010. ACM.
20. J. Park and R. Sandhu. Towards usage control models: beyond traditional access control. In *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies*, pages 57–64, New York, NY, USA, 2002. ACM.
21. C. Skalka, X. S. Wang, and P. Chapin. Risk management for distributed authorization. *J. Comput. Secur.*, 15(4):447–489, 2007.
22. K. Stolen, F. den Braber, T. Dimitrakos, R. Fredriksen, B. A. Gran, S.-H. Houmb, M. S. Lund, Y. Stamatiou, and J. O. Aagedal. Model-based risk assessment - the coras approach. In *Proceedings of the Norsk Informatikkkonferanse*, pages 239–249. Tapir, 2002.
23. G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical Report 800-30, National Institute of Standards and Technology, 2001. available via `http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf` on 13/05/2009.
24. H. C. Tijms. *A First Course in Stochastic Models*. Wiley, 2003.
25. L. Wang, D. Wijesekera, and S. Jajodia. A logic-based framework for attribute based access control. In *Proceedings of the 2004 ACM workshop on Formal methods in security engineering (FMSE'04)*, pages 45–55, New York, NY, USA, 2004. ACM.
26. L. Zhang, A. Brodsky, and S. Jajodia. Toward information sharing: Benefit and risk access control (barac). In *Proceedings of the 7th International Workshop on Policies for Distributed Systems and Networks*, pages 45–53, Washington, DC, USA, 2006. IEEE Computer Society.