Risk-based Approach: A New Perspective on Declassification and Endorsement

Yunchuan GUO, Lihua YIN
Institute of Information Engineering
Chinese Academy of Sciences
guoyunchuan@nelmail.iie.ac.cn

Liang CHANG
Guangxi Key Laboratory of Trusted Software
(Guilin University of Electronic Technology)
Guilin, China

Athanasios V. Vasilakos
Dept of Computer and
Telecommunications Engineering
University of Western Macedonia
Kozani, Greece

Abstract—Declassification and endorsement can efficiently improve the usability of applications, some *declassify* and *endorse* operations in practice, however, are often ad-hoc and nondeterministic. In this poster, we introduce risk assessments into the declassification and endorsement. Because risk assessments have explicit security conditions and results, our approach can solve the *ad-hoc* and *nondeterministic* semantics problem and builds a bridge between risk assessments and declassification/ endorsement.

Keywords—Declassification; Endorsement; Risk assessment

I. INTRODUCTION

Generally, a natural protection against security risks is to enforce confidentiality and integrity, that is, to ensure that confidentiality and integrity are satisfied. To achieve this goal, a large number of efforts are spent in both academia and industry, an important one of which is non-interference: a guarantee that any sequence of low inputs will produce the same low outputs, regardless of what the high level inputs are. Although non-interference has been widely discussed both at the language level and at the operating-system level, it is too rigid to be used in practice: many applications have to violate the non-interference policy. In order to reliably implement non-interference policy, declassification and endorsement are respectively proposed to control which information can be intentionally released and which untrusted information can be intentionally used. These two approaches, which relax confidentiality policies and integrity policies respectively, efficiently improve applications' flexibility and are widely used in realistic applications, such as JIF and web applications. Obviously, reliability of these applications severely depends on the security of declassification and endorsement.

Motivation: Existing work for declassification and endorsement often suffers from the problem of security conditions[1]: the semantics of the *declassify* and *endorse* operations are ad-hoc, speculative and nondeterministic. Evenly, some *declassify* and *endorse* operations in practice are often insecure. These insecure operations will severely violate confidentiality and integrity. Thus, it is necessary to design a reliable approach to declassify and/or endorse information.

Our approach and contributions: In order to solve the above problem, we study declassification and endorsement from a new perspective of risk assessments. Intuitively, when relaxing confidentiality policies and/or integrity policies, we respectively assess risks brought by performing these two relaxes. If these risks are acceptable, the *declassification* and/or *endorsement* operations are executed; Otherwise, they are denied. Because risk assessments have explicit security conditions and results, our approach can solve the *ad-hoc* and *nondeterministic* semantics problem which often happens in existing approaches. To the best of our knowledge, no work links risk assessments to declassification and endorsement to date, our work builds a bridge between risk assessments and declassifications/endorsements.

II. RISK-BASED DECLASSIFICATION AND ENDORSEMENT

Let *s* and *i* denote security labels for confidentiality and integrity, respectively. Subscripts *l* and *h* represent a lower level and a higher level, respectively. For example, s_h and s_l may be a *secret* label and a *public* label, respectively. i_h and i_l may be a *untrust* label and a *trust* label, respectively. We define the ordering $\preceq$ between s_h *and* s_l as $s_l \preceq s_h$ and between i_h *and* i_l as $i_h \preceq i_l$. When both confidentiality and integrity are considered for applications, we can compose confidentiality labels and integrity labels as tuple label (*s*,*i*). Let *T* be a set of all tuple labels. Generally, the ordering on (*s*,*i*) forms a lattice and an example is shown in Fig 1.

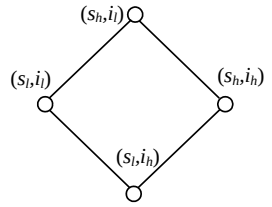

Figure 1. Information Flow Lattice

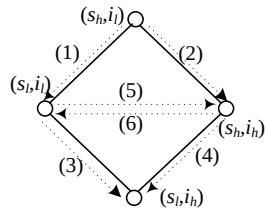

Figure 2. Risks caused by declassification/endorsement

Given process u with securty label (s_u, i_u), process u' with label $(s_{u'}, i_{u'})$ and let $u \rightarrow u'$ denote that information from u flows into u'. If $s_u \prec s_{u'}$, then we need declassify u; and if $i_u \prec i_{u'}$, then we need endorse u. For simplicity, we call these two kinds of operations as label castings. Although enforcing label castings to provide support for flexible decision-making, risks always exist during castings, because these might incorrectly change some labels. Let $u : (s_u, i_u) \rightsquigarrow u' : (s_{u'}, i_{u'})$ denote the casting from u with label (s_u, i_u) to u' with $(s_{u'}, i_{u'})$. In the sequence, u and u' is also called *sources* and *destinations*, respectively. Formally, we define *risks* as follows.

Definition 1. There exist risks in the label casting $u : (s_u, i_u) \rightsquigarrow u' : (s_{u'}, i_{u'})$, if $(s_u, i_u) \not\preceq u' : (s_{u'}, i_{u'})$.

In another words, any attempt of casting label (s_u, i_u) into $(s_{u'}, i_{u'})$ may cause a risk, if either $(s_{u'}, i_{u'}) \prec (s_u, i_u)$ or (s_u, i_u) is not comparable with $(s_{u'}, i_{u'})$. In [2], a risk is defined as: a risk exists if the subject with a low security level is able to access an object with a high level. This definition is suitable for total orders on security levels, but is inappropriate for lattices (since type castings under incomparable types are also considered in our order-based threats). For example, in the above lattice, the six castings represented by dotted arrows will cause risks, as shown in Figure 1. Note: the castings labeled with (5) and (6) will also bring risks because these two labels are not mutually comparable.

Definition 2. *Risk index* is a binary function $RI : T \times T \rightarrow [0, \infty]$ for representing the degree of risks caused by type castings. Intuitively, TI should (partially) hold the following properties.

(1) RI should satisfy the *separation* axiom and *coincidence* axiom.

(2) For comparable elements $t_1, t_2 \in T$, RI should satisfy the *non-symmetry* axiom.

If any two tuple labels t_1 and t_2 are comparable, then we use the following formula (similar to [2,3]) to measure their *RI*.

$$RI(t_1, t_2) = \begin{cases} a^{\omega \times level(t_1) - level(t_2)} & if \quad t_1 > t_2 \\ 0 & otherwise \end{cases}$$

where function $level$, mapping basic labels to real numbers and represents the degree of a label restriction, $a, \omega \geq 0$. If two labels are not comparable with, the above approach is unsuitably adopted. To solve this problem, two policies are proposed as follows.

Down-up policy. Given a casting $u : (s_u, i_u) \rightsquigarrow u' : (s_{u'}, i_{u'})$, the down-up policy first computes the greatest label (s, i) with the constraints: (1) (s_u, i_u) is more restrictive than (s, i), i.e. $(s, i) \preceq (s_u, i_u)$ and (2) $(s_{u'}, i_{u'})$ is more restrictive than(s, i), i.e. $(s, t) \preceq (s_{u'}, i_{u'})$ (Because $(T, \preceq)$ is a lattice, the greatest type of satisfying these two constraints always exists), and then evaluates *risk index* caused by casting (s_u, i_u) to (s, i) (Because (s_u, i_u) and (s, i) are comparable, we can adopt the approaches based on the above approach to assess RI). Finally, this RI is used as the risk index of casting (s_u, i_u) to $(s_{u'}, i_{u'})$ for the down-up policy.

Figure 3 gives an intuitive explanation for this policy. In Figure 3, type (s_u, i_u) is not comparable with $(s_{u'}, i_{u'})$, and (s, i) is the greatest element with $(s, i) \preceq (s_u, i_u)$ and $(s, t) \preceq (s_{u'}, i_{u'})$. As a result, $RI((s_u, i_u), (s, t))$ is regarded as the risk index of casting (s_u, i_u) to $(s_{u'}, i_{u'})$.

The ground of this assessment is as follows: in the first constraint of this policy, risks exist for casting (s_u, i_u) to (s, i) because(s_u, i_u) is more restrictive than (s, i); In the second constraint, the case that $(s_{u'}, i_{u'})$ is more restrictive than (s, i)) means that no risk exists when information flows from (s, i) to $(s_{u'}, i_{u'})$. As a result, from the perspective of the lower semi-lattice, the maximal risk index caused by the casting from (s_u, i_u) to $(s_{u'}, i_{u'})$ is the risk index brought by casting from (s_u, i_u) to(s, i). That is, $RI((s_u, i_u), (s, t))$ can be regarded as the risk index of casting (s_u, i_u) to $(s_{u'}, i_{u'})$.

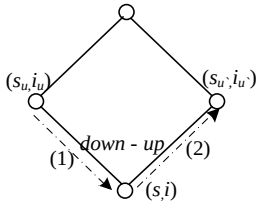

Figure 3. Down-up policy

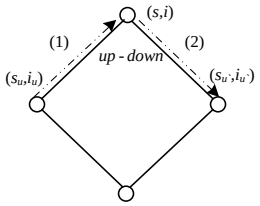

Figure 4. Up-down policy

Up-down policy: The policy is similar to the down-up policy, and Figure 4 gives an intuitive example for this policy.

Generally, risks should monotonically increase with the risk index. Although there could be many approaches to convert the risk index to a risk value, in our work logistic functions are chosen because its every parameter owns an explicit means and the requirements of the different application contexts in castings can be satisfied by tuning the parameters of logistic functions. For example, Figure 5 gives the risk values caused by castings a higher confidentiality label to a lower label, where points on the *X* axis denote castings, for example, (2→1) means that confidentiality label with level 2 is casted into level 1. As shown in Figure 5, the higher the level of sources is, the higher risks are, and once the level of sources is given, the risk increases with the decrease of the level of destinations. This is completely consistent with our expectation.

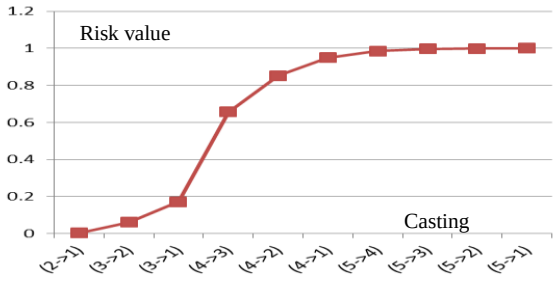

Figure 5. Example of computing the likelihood of risks

So, before performing the *declassify and/or endorsement* operation, we first evaluate the risk caused by the operation(s). if a risk is less than a given threshold, then the operation(s) can be securely performed.

III. FUTURE WORK

Our work builds a bridge between risk assessments and declassifications/endorsements. In the future work, we will integrate our approach to various applications, such as JIF. Additionally, we will also study how the accuracy of risk assessments is improved.

[1]. Askarov A, Myers A. A semantic framework for declassification and endorsement. Programming Languages and Systems. 2010:64-84.

[2]. Khambhammettu H, Boulares S, Adi K, Logrippo L. A Framework for Risk Assessment in Access Control Systems, Computers & Security. 2013: 86-103.

[3]. Cheng P, Rohatgi P, Keser C, Wagner G, Reninger A. Fuzzy Multi–Level Security: An Experiment on Quantified Risk–Adaptive Access Control. IEEE Symposium on Security and Privacy. 2007: 222-230.