A Framework for Risk Assessment in Access Control Systems ☆

Hemanth Khambhammettu[a], Sofiene Boulares[b], Kamel Adi[b], Luigi Logrippo[b]

[a] *PricewaterhouseCoopers LLP, New York, NY, USA*
[b] *Université du Québec en Outaouais, Gatineau, Québec, Canada*

Abstract

We describe a framework for risk assessment specifically within the context of risk-based access control systems, which make authorization decisions by determining the security risk associated with access requests and weighing such security risk against operational needs together with situational conditions. Our framework estimates risk as a product of threat and impact scores. The framework that we describe includes four different approaches for conducting threat assessment: an object sensitivity-based approach, a subject trustworthiness-based approach and two additional approaches which are based on the difference between object sensitivity and subject trustworthiness. We motivate each of the four approaches with a series of examples. We also identify and formally describe the properties that are to be satisfied within each approach. Each of these approaches results in different threat orderings, and can be chosen based on the context of applications or preference of organizations. We also propose formulae to estimate the threat of subject-object accesses within each of the four approaches of our framework.

We then demonstrate the application of our threat assessment framework for estimating the risk of access requests, which are initiated by subjects to perform certain actions on data objects, by using the methodology of NIST Special Publication 800-30. We show that risk estimates for access requests actually differ based on the threat assessment approach that has been chosen. Therefore, organizations must make prudent judgement while selecting a threat assessment function for risk-based access control systems.

Keywords: Security, Access control, Risk, Threat, Impact

1. Introduction

The "need to share" information in dynamic environments has prompted the development of risk-based access control systems [1, 2, 3, 4, 5, 6]. Essentially, in order to facilitate information sharing, risk-based access controls extend traditional access control paradigms to provide support for flexible decision-making by specifying acceptable security

☆This paper is an extended version of our paper entitled "A framework for threat assessment in access control systems" that appeared in Proceedings of 27th IFIP TC 11 Information Security and Privacy Conference (SEC 2012), 2012.

*Corresponding author: Hemanth Khambhammettu, Email: hemanth.khambhammettu@us.pwc.com

risk, operational needs and situational conditions [4]. Risk-based access control mechanisms make access decisions by determining the security risk associated with access requests and weighing such security risk against operational needs together with situational conditions. Specifically, an access request will be *permitted* if the operational benefits outweigh the security risk of granting access to information, and *denied* otherwise.

Clearly, computing the security risk of access requests is an important aspect of risk-based access control systems. However, determining security risk is a complex task, which requires the consideration of a variety of factors, such as the trustworthiness of subjects (or users), sensitivity of data, type of access being requested, access history of subjects and objects, physical or logical location or device from which access to data is being requested as well as protection capabilities and robustness of the system that maintains data [4]. Furthermore, the interpretation and computation of security risk might differ based on the context of applications or culture of organizations.

The NIST Special Publication (SP) 800-30 [7] is a well-known "*risk management*" standard for enterprise systems. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level [7]. The NIST SP 800-30 provides a foundation for the development of an effective risk management program and aims to help organizations to better manage IT-related mission risks. Recently, NIST published a revised version of this standard (referred to as "NIST SP 800-30 Revision 1") that focuses on the "*risk assessment*" component of risk management [8]. Risk assessment is the process of identifying, estimating, and prioritizing information security risks. The NIST SP 800-30 [7] computes risk as a product of threat likelihood and impact values. Although this formula has not been explicitly repeated in the revised publication [8], the notions of risk in both [7] and [8] are essentially the same.

Note that the NIST SP 800-30 [7] and NIST 800-30 Revision 1 [8] provide no concrete suggestions for estimating threats that subjects present towards data objects. Furthermore, none of the existing work on estimating risk of access requests [9, 2, 5, 6] has explicitly provided different approaches to estimate threats that subjects may present towards data objects or to compute risk estimates of actions that subjects may perform on data objects.

In this paper, we first focus on estimating the threats that subjects may present towards objects and, subsequently, develop different approaches to compute risk estimates of access requests. In particular, our framework offers different approaches to estimate such threats which could be applied based on the context of applications.

Consider, for example, a business-to-business scenario that enables organizations to successfully execute their missions, which require subjects (or users) from both intra-business and inter-business to access sensitive data.

- Assume that access requests for sensitive data objects have been initiated by subjects who are employees of the business that owns the requested data objects. In other words, access requests are initiated by subjects who are directly known to (and trusted to some degree by) the system. In such situations, data owners might be more concerned about the sensitivity of data being requested than the trustworthiness of subject. Hence, sensitivity of data objects may be more important than trustworthi-

ness of subjects for estimating the threats posed by subjects towards objects.

- Alternatively, assume that access requests for sensitive objects have been initiated by subjects who are employed by business partners. In other words, subjects who initiate access requests may not be (directly) known to data owners. In such situations, data owners might be greatly concerned about the trustworthiness of subjects for granting access to the requested data objects. Consequently, trustworthiness of subjects may be more important than sensitivity of data objects while estimating the threats posed by subjects towards objects.

Towards this end, we have focused our efforts on developing a suite of threat assessment techniques by considering the sensitivity of objects and trustworthiness of subjects. Of course, as mentioned earlier, we may have to consider a variety of additional factors to compute threat metrics in a comprehensive manner. Nevertheless, even by only considering trustworthiness of subjects and sensitivity of objects, our framework provides significant insights into various ways for assessing the threats posed by subjects towards objects.

We also show that the threat assessment techniques presented in this paper can be used to compute risk metrics according to Formula 2 that is given above.

The following are the main contributions of this paper.

- We present a family of approaches for assessing the threats posed by subjects towards objects: an object sensitivity-based approach, a subject trustworthiness-based approach and two additional approaches which are based on the difference between object sensitivity and subject trustworthiness. We use a series of examples as a basis for developing and identifying the properties of our threat assessment approaches, which provide support for *qualitative* threat assessment of subject-object accesses. Each of these approaches results in different threat orderings, and can be chosen based on the context of applications or preference of organizations.

- We demonstrate that the order in which "general threat principles" (described in Section 3.2) are applied makes a difference in the resulting threat vectors.

- We also propose formulae which satisfy the properties of each approach for quantitatively measuring the threat of subject-object accesses.

- We describe an approach for estimating the impact of performing certain actions on data objects in terms of information security objectives that include *confidentiality*, *integrity* and *availability*.

- We show the application of our threat and impact assessment framework for computing risk of access requests by considering the NIST SP 800-30 methodology. In particular, we demonstrate that risk estimates for access requests differ based on the threat assessment approach that has been chosen.

The rest of the paper is organized as follows. In Section 2, we briefly describe the risk assessment methodology of the NIST Special Publication 800-30 and define a risk assessment

function for access control systems. Section 3 describes our threat assessment framework. We propose formulae for quantifying threat assessment in Section 4. Section 5 describes the computation of impact scores and the application of our threat assessment framework with the NIST Special Publication 800-30 for quantifying risk of access requests. We compare our work with notable works of the literature in Section 7. We draw conclusions for this paper and outline future research directions in Section 8.

2. Overview of the NIST SP 800-30 Standard

The NIST SP 800-30 [7] standard provides a foundation for developing a risk management program. As mentioned earlier, a revised version of this standard has recently been published [8] that focuses on the *risk assessment* component of risk management and the notions of risk in both [7] and [8] are essentially the same.

In this paper, we adopt the risk assessment function proposed in the NIST SP 800-30 [7] for computing risk scores based on our threat and impact assessment approaches.

> "Risk *is a function of the likelihood of a given threat-sources exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." [7]*

Essentially, risk scores are computed based on inputs from threat likelihood and threat impact on data. More specifically, risk scores are computed as a product of threat likelihood values and impact values on data should the threat be successfully exercised. The risk assessment function of NIST SP 800-30 [7] is as follows:

$$Risk = \texttt{threat likelihood value} \times \texttt{impact value}. \tag{1}$$

We adopt the above shown NIST SP 800-30 risk assessment function to develop a risk assessment function for access control systems that will be used in this paper. Specifically, the risk of permitting a subject $s \in S$ to perform an action $a \in A$ on an object $o \in O$ is given by the following function:

$$Risk(s, o, a) = \texttt{Threat}(s, o) \times \texttt{Impact}(o, a). \tag{2}$$

where $\texttt{Threat}(s, o)$ represents the threat that a subject (threat source) s may present towards an object (threat target) o and $\texttt{Impact}(o, a)$ represents the adverse impact on the satisfaction of security objectives that results from successfully performing action a on o.

It is clear that any implementation of the threat function must meet the following requirements:

- **Property A:** Threat is proportional to the value of information contained within objects.
- **Property B:** Threat is inversely proportional to the value and the importance of users within the organization.

In our proposition, the value of information contained within objects is encoded by sensitivity scores and the value and importance of users is encoded by trustworthiness scores.

3. A Framework for Assessing "Threat"

It is clear from Formula 2 that computing threat scores is a prerequisite to compute risk scores. Hence, in this section, we first develop our framework for assessing the threat of subject-object accesses within the context of access control systems by considering object sensitivity and subject trustworthiness. Throughout this section, we present a series of examples for developing the conceptual underpinnings of our threat assessment approaches. (We discuss the computation of impact scores and risk scores in Section 5.)

3.1. Assumptions

We assume the existence of the following entities within an access control system: a set of subjects S and a set of objects O and a set of actions A. Furthermore, we assume that every object is associated with a sensitivity score that best reflects the protection needs of the data it holds. Typically, sensitivity scores are assigned to data objects by data owners. We also assume that every subject is associated with a trustworthiness score that best reflects the trust bestowed upon the subject by the organization that owns the data. Such trustworthiness scores of subjects may be computed by referring to attributes and/or access histories of subjects. A function $ol : O \rightarrow \mathbb{N}$ formally represents the assignment of sensitivity scores to objects, where $\mathbb{N} = \{0, 1, 2, \ldots\}$. A function $sl : S \rightarrow \mathbb{N}$ formally represents the assignment of trustworthiness scores to subjects.

We assume a "risk-based" system where a subject labeled to a certain trustworthiness score is *always* permitted to access objects whose sensitivity is up to that score. In other words, all accesses initiated by a subject $s \in S$ to an object $o \in O$, such that $sl(s) \geqslant ol(o)$, will be *permitted*. However, should $sl(s) < ol(o)$ then access decisions are made by the system by computing the risk of granting access to o for s and referring to the risk acceptance level specified within the access control policy. In particular, an access request initiated by a subject $s' \in S$ to object o, such that $sl(s') < ol(o)$, will be *permitted* if the risk of granting access to o for s' is lower than the specified acceptable risk threshold, and *denied* otherwise.

3.2. Defining "threat"

As discussed earlier in Section 1 and also shown above in Formula 2, threat metrics are a pre-requisite to compute risk metrics. We take the point of view that permitting a subject s to access an object o, such that $sl(s) < ol(o)$, presents by itself a "measurable threat", independently of what might happen to the information that is accessed. In this section, we define the notion of "threat" in the context of the right to access objects by subjects. In particular, threat of subject-object accesses is defined as follows.

Definition 1. *We say that there exists a* threat *if a subject $s \in S$ is able to access an object $o \in O$, such that $sl(s) < ol(o)$.*

In other words, any attempt by a subject s to access an object o, such that $sl(s) \geqslant ol(o)$ does not present a threat.

Intuitively, any measure of threat is affected by one or more of the following three general principles:

- **Principle 1:** Threat increases as object sensitivity score increases.
- **Principle 2:** Threat increases as subject trustworthiness score decreases.
- **Principle 3:** Threat increases as the difference between the object sensitivity score and subject trustworthiness score increases.

We define a function $\texttt{Threat} : S \times O \rightarrow [0, 1]$ that represents the threat value of a subject $s \in S$ accessing an object $o \in O$. We use relation $\preccurlyeq^{\texttt{T}}$ to denote an ordering that represents threat on a set of subject-object accesses. In particular, $\preccurlyeq^{\texttt{T}}$ can be defined in terms of subject-object accesses in the following way: $(s, o) \preccurlyeq^{\texttt{T}} (s', p')$ iff $\texttt{Threat}(s, o) \leqslant \texttt{Threat}(s', o')$.

The relation $\preccurlyeq^{\texttt{T}}$ allows threats to be compared, and "greater" and "lesser" threats assessed. We define $(s, o) \simeq^{\texttt{T}} (s', o')$ iff $(s, o) \preccurlyeq^{\texttt{T}} (s', o')$ and $(s, o) \succcurlyeq^{\texttt{T}} (s', o')$, and say (s', o') is a greater threat than (s, o) and write $(s, o) \prec^{\texttt{T}} (s', o')$ if $(s, o) \preccurlyeq^{\texttt{T}} (s', o')$ and $(s, o) \not\simeq^{\texttt{T}} (s', o')$. We may write $(s', o') \succ^{\texttt{T}} (s, o)$ whenever $(s, o) \prec^{\texttt{T}} (s', o')$.

3.3. Running example

In this section, we describe the setting of a scenario that is used in the rest of the paper for motivating our threat assessment approaches.

We assume the existence of the following four subjects: `Alice`, `Bob`, `Carol` and `Dave`. Table 1(a) illustrates the trustworthiness scores of these four subjects.

Let us consider two objects o and o' within a military context, such that o maintains information regarding the `location` for nuclear weapons and o' maintains `launch codes` for nuclear weapons. It is reasonable to assume here that information regarding the `launch codes` for nuclear weapons is *more sensitive* than the `location` of nuclear weapons. Hence, we assume that object o is assigned a sensitivity score 90 and object o' is assigned a sensitivity score 100. Table 1(b) shows the sensitivity scores of objects o and o'.

Recall that the objective of our work is to assess the threat of access requests, where a subject $s \in S$ who initiated the request may not be pre-authorized for the requested data object $o \in O$. Hence, throughout this paper, we only cite examples where $sl(s) < ol(o)$.

3.4. Object-based threat assessment

It is possible that certain applications which maintain "highly" sensitive data, such as government or military systems, may understand or interpret threat in terms of access to such data. We now give examples that motivate our technique for threat assessment that primarily is based on the sensitivity score of objects.

Example 1. *Suppose that* `Alice` *requests access to object* o'*, and* `Bob` *requests access to object* o*. We have the following from Table 1:* $sl(\texttt{Alice}) = 90$*,* $sl(\texttt{Bob}) = 80$*,* $ol(o) = 90$ *and* $ol(o') = 100$*.*

If we were to consider object sensitivity score *to be the basic criteria for determining threat measures, then according to Principle 1 stated in Section 3.2 allowing* `Alice` *to access object* o' *is a* greater threat *than allowing* `Bob` *to access object* o*. This is because the sensitivity score of object* o' *is* higher *than the sensitivity score of object* o*.*

In the above example, we were able to understand which access poses a greater threat by simply comparing the sensitivity scores of those two objects. However, as we show below, such a technique is no longer sufficient when object sensitivity scores are the same.

Example 2. *Let us extend Example 1 by considering an additional subject* `Carol` *whose trustworthiness score is given in Table 1 as follows:* $sl(\texttt{Carol}) = 70$. *Suppose that* `Carol` *requests access to object* o', *where* $ol(o') = 100$. *In other words, both* `Alice` *and* `Carol` *request access to object* o'.

Now, if we were to determine which of these two accesses is a greater threat, then according to Principle 2 (see Section 3.2) one is likely to conclude that allowing `Carol` *to access object* o' *is a* greater threat *than allowing* `Alice` *to access* o'. *This is because* `Carol` *who has a trustworthiness score of* 70 *is* less trusted *than* `Alice` *who has a trustworthiness score of* 90.

Remark 1 (from Examples 1 and 2)**.** *A threat assessment technique that primarily is based on* object-sensitivity scores *should support the following:*

1. always *apply Principle 1 (that is, threat always increases as object sensitivity score increases),*

2. whenever object sensitivity scores are the same*, apply Principle 2 (that is, threat increases as subject trustworthiness score decreases).*

Based on Remark 1, we obtain the following ordering of threat for the accesses which were considered in Examples 1 and 2: $(\texttt{Bob}, o) \prec^{\texttt{T}} (\texttt{Alice}, o') \prec^{\texttt{T}} (\texttt{Carol}, o')$.

It can easily be seen that we can construct a "priority order" of excessive accesses by subjects for objects, when sensitivity scores are higher than trustworthiness scores, in terms of their threat by adhering to the properties of Remark 1. Essentially, the properties of Remark 1 can be generalized as follows: $(s, o) \prec^{\texttt{T}} (s', o')$ if either

1. $ol(o) < ol(o')$ or

2. $ol(o) = ol(o')$ and $sl(s') < sl(s)$.

Within an object-based threat assessment approach, whenever object sensitivity scores are the same, unlike Remark 1 we may wish to apply Principle 3 as a secondary criterion. In other words, we may use "the difference of object sensitivity and subject trustworthiness scores" as a secondary parameter, rather than subject trustworthiness scores. Note however that whenever the object sensitivity score is fixed, the difference between object sensitivity and subject trustworthiness scores increases only if subject trustworthiness scores decrease. This means that the threat priority order remains the same irrespective of whether we apply Principle 2 or Principle 3 as a secondary criterion. Hence, we do not describe the subcase that applies Principle 3 as a secondary criterion.

3.5. Subject-based threat assessment

As discussed earlier in Section 1, in certain scenarios (such as business-to-business environments), access requests could be initiated by subjects who may not be (directly) known to data owners. In such situations, trustworthiness of subjects may take higher preference than sensitivity of data objects while estimating access threats.

We now give examples that motivate our technique for threat assessment that, primarily, is based on trustworthiness scores of subjects.

Example 3. *Let us reuse the setting of Example 1 here. That is, we consider subjects* `Alice` *and* `Bob`*, and suppose that* `Alice` *requests access to object o', and* `Bob` *requests access to object o.*

Now, should subject trustworthiness score *be the basic criteria for conducting threat assessment, then according to Principle 2 (see Section 3.2) one is likely to conclude that granting access to* `Bob` *for object o is a* greater threat *than granting access to* `Alice` *for o'. This is because* `Bob`*, who has a subject trustworthiness score of* 80*, is* less trusted *than* `Alice`*, who has a subject trustworthiness score of* 90*.*

Example 4. *Let us extend Example 3 by considering an additional user* `Dave` *where $sl($*`Dave`*$) = 80$ (see Table 1(a)). Now both* `Bob` *and* `Dave` *have the same trustworthiness score. Suppose that* `Dave` *is requesting access to object o'.*

Now, if we were to determine which one of the above two accesses of `Bob` *and* `Dave` *poses a greater threat, then according to Principle 1 (see Section 3.2) we may reasonably say that granting access to* `Dave` *for o' is a* greater threat *than granting access to* `Bob` *for o. This is because– although both* `Bob` *and* `Dave` *have the same trustworthiness scores–* `Dave` *is requesting access to object o' which has a* higher *sensitivity score than object o that* `Bob` *is requesting access to.*

Remark 2 (from Examples 3 and 4)**.** *A threat assessment technique that primarily is based on* subject-trustworthiness scores *should support the following properties:*

1. always *apply Principle 2 (that is, threat increases as subject trustworthiness score decreases),*

2. whenever subject trustworthiness scores are the same*, apply Principle 1 (that is, threat increases as object sensitivity score increases).*

Based on Remark 2, we obtain the following ordering of threat for the subject-object accesses which were considered in Examples 3 and 4: $(\texttt{Alice}, o') \prec^{\texttt{T}} (\texttt{Bob}, o) \prec^{\texttt{T}} (\texttt{Dave}, o')$.

Essentially, the properties of Remark 2 can be generalized as follows: $(s, o) \prec^{\texttt{T}} (s', o')$ if either

1. $sl(s') < sl(s)$ or

2. $sl(s') = sl(s)$ and $ol(o') > ol(o)$.

It is important to note the effect of the basic criterion on threat orderings or metrics when subjects request access to objects, where sensitivity scores are higher than trustworthiness scores. In particular, should the sensitivity score of objects be the basic criterion for assessing threat, then $(\texttt{Bob}, o) \prec^{\mathsf{T}} (\texttt{Alice}, o')$ (see Example 1). Whereas, if the trustworthiness score of subjects is considered as the basic criterion for assessing threat, then $(\texttt{Alice}, o') \prec^{\mathsf{T}} (\texttt{Bob}, o)$ (see Example 3).

Note that, whenever subject trustworthiness scores are the same, unlike Remark 2 we may wish to apply Principle 3 as a secondary criterion. That is, we may wish to use "the difference of object sensitivity and subject trustworthiness scores" as a secondary parameter, rather than object sensitivity scores. However, note that whenever the subject trustworthiness score is fixed, the difference between object sensitivity and subject trustworthiness scores increases only if object sensitivity scores increase. This means that, within a subject-based threat assessment approach, the threat priority order remains the same irrespective of whether we apply Principle 1 or Principle 3 as a secondary criterion. Hence, we do not describe the subcase that applies Principle 3 as a secondary criterion.

3.6. Difference of scores-based threat assessment

In certain scenarios, we may not be directly concerned with either the object sensitivity scores or subject trustworthiness scores; however, our objective could be to understand threat simply in terms of the difference between object sensitivity and subject trustworthiness scores. Essentially, in such an approach, the degree of threat proportionally increases with the difference between object sensitivity and subject trustworthiness scores.

In this section, we adopt such a notion of threat (as described above) and develop two different techniques for threat assessment which, primarily, are based on the difference between the sensitivity scores of objects and subjects. We first give examples below for motivating our threat assessment techniques and then formalize their properties.

Example 5. *Let us reuse the setting from Examples 1 and 2 here. In particular, we consider user* Bob *from Example 1 and* Carol *from Example 2. As before, we suppose that* Bob *requests access for object o and* Carol *requests access for object o'.*

Now, should the basic criteria for determining threat measures be the difference between object sensitivity and subject trustworthiness scores*, then according to Principle 3 (see Section 3.2) granting access to* Carol *for object o' is a* greater threat *than granting access to* Bob *for object o. This is because the difference between the sensitivity score of object o and trustworthiness score of* Carol *(which is $100 - 70 = 30$) is* greater *than the difference between the sensitivity score of object o' and trustworthiness score of* Bob *(which is $90 - 80 = 10$).*

Note, in the above example, that the differences between object sensitivity and subject trustworthiness scores for the two accesses under consideration are not the same. Hence, we were able to compare the threat of granting accesses by simply computing and comparing the difference between object sensitivity and subject trustworthiness scores of those two subject-object accesses.

We show in the following example that such a technique is no longer sufficient when the difference between object sensitivity and subject trustworthiness scores of subject-object accesses is the same.

Example 6. *Let us extend Example 5 by also considering subject* `Alice`*. As before, we suppose that* `Alice` *requests access for object* o'*, where* $sl(\texttt{Alice}) = 90$ *and* $ol(o') = 100$ *(see Table 1).*

Note that the difference between the sensitivity score of object o' *and trustworthiness score of* `Alice` *(which is* $100 - 90 = 10$*)*– is the same as– *the difference between the sensitivity score of object* o *and trustworthiness score of* `Bob` *(which is* $90 - 80 = 10$*). Hence, it is not immediately obvious which of the above two subject-object accesses poses a greater threat.*

If we were to determine which of the two subject-object accesses considered in Example 6 is a greater threat, then we may choose between applying either Principle 1 or Principle 2 (see Section 3.2) yielding two different approaches, which consider different secondary parameters, for resolving the parity observed in Example 6. These two approaches are described below.

3.6.1. Difference weighted by object sensitivity score

In this approach, we consider object sensitivity scores as a secondary criterion and apply Principle 1 which says that threat increases with an increase in object sensitivity scores (see Section 3.2) for resolving the parity observed in Example 6.

This means that, in Example 6, granting access to object o' for `Alice` is a *greater threat* than granting access to object o for `Bob`, because $ol(o') > ol(o)$.

Remark 3. *A threat assessment technique that primarily is based on* the difference between object sensitivity and subject trustworthiness scores*, and that uses* object sensitivity scores *as a secondary criterion should support the following properties:*

1. always *apply Principle 3 (that is, threat increases as the difference between object sensitivity and subject trustworthiness scores increases),*

2. whenever parity is observed on the difference between object sensitivity and subject trustworthiness scores*, apply Principle 1 (that is, threat increases as object sensitivity score increases).*

Based on Remark 3, we obtain the following ordering of threat for the subject-object accesses which were considered in Examples 5 and 6: $(\texttt{Bob}, o) \prec^{\texttt{T}} (\texttt{Alice}, o') \prec^{\texttt{T}} (\texttt{Carol}, o')$.

The properties of Remark 3 can be generalized as follows: $(s, o) \prec^{\texttt{T}} (s', o')$ if either

1. $(ol(o) - sl(s)) < (ol(o') - sl(s'))$ or

2. $(ol(o) - sl(s)) = (ol(o') - sl(s'))$ and $ol(o') > ol(o)$.

3.6.2. Difference weighted by subject trustworthiness score

In this approach, we consider subject trustworthiness scores as a secondary criterion and apply Principle 2 which says that threat increases with a decrease in subject trustworthiness scores (see Section 3.2) for resolving the parity observed in Example 6.

Recall from Example 6 that the difference between the sensitivity score of object o' and trustworthiness score of `Alice` (which is $100 - 90 = 10$)– *is the same as*– the difference between the sensitivity score of object o and trustworthiness score of `Bob` (which is $90-80 = 10$). In this approach, granting access to object o `Bob` poses a *greater threat* than granting access to object o' `Alice`, because $sl(\texttt{Bob}) < sl(\texttt{Alice})$.

Remark 4. *A threat assessment technique that primarily is based on* the difference between object sensitivity and subject trustworthiness scores*, and that uses* the subject trustworthiness scores *as a secondary criterion should support the following properties:*

1. always *apply Principle 3 (that is, threat increases as the difference between object sensitivity and subject trustworthiness scores increases),*
2. whenever parity is observed on the difference between object sensitivity and subject trustworthiness scores*, apply Principle 2 (that is, threat increases as subject trustworthiness score decreases).*

Based on Remark 4, we obtain the following ordering of threat for the subject-object accesses which were considered in Examples 5 and 6: $(\texttt{Alice}, o') \prec^{\texttt{T}} (\texttt{Bob}, o) \prec^{\texttt{T}} (\texttt{Carol}, o')$.

The properties of Remark 4 can be generalized as follows: $(s, o) \prec (s', o')$ if either

1. $(ol(o) - sl(s) < ol(o') - sl(s'))$ or
2. $(ol(o) - sl(s) = ol(o') - sl(s'))$ and $sl(s') < sl(s)$.

4. Formulae for Quantifying Threat

In the previous section, we have described four different approaches for threat assessment and defined the properties that are to be satisfied within each approach. We have also discussed the construction of "threat priority orders" for a given set of subject-object accesses in all four approaches that we developed.

Such priority orders only offer a qualitative threat comparison between two or more subject-object accesses. For example, given two subject-object accesses (s, o) and (s', o'), a threat priority order is useful to determine which one of the given subject-object accesses poses a greater threat than the other.

For computational purposes, quantitative measures which correspond to this threat ordering may be useful. However, there can be many different formulae which respect the properties of the four approaches and can quantitatively measure the threat of granting access to a subject s for an object o within each approach, where $sl(s) < ol(o)$. In this section, we propose one such formula for each approach and describe their construction.

In the rest of the paper, for the purposes of generality, we use the terminology of "subject clearance levels" which represent trustworthiness scores of subjects and "object classification levels" which represent sensitivity scores of objects.

Threat Index. We now introduce the concept of threat indexing of subject clearance levels and object classification levels. Essentially, we assign a unique numerical value from the set $\{0, \ldots, |L| - 1\}$ that represents the threat index of a security level $l \in L = \{\mathsf{Unclassified}, \mathsf{Restricted}, \mathsf{Classified}, \mathsf{Secret}, \mathsf{TopSecret}\}$.

- Note that, from the point of view of subjects, we expect the threat to increase as subject clearance levels decrease. For example, a subject who holds a Classified clearance level poses a greater threat than a subject who holds a Secret clearance level.

  Hence, subject threat index values decrease with subject clearance levels. We write $\widehat{l}$ to denote a subject threat index. Formally, $\widehat{l} = |L| - l$. The second column of Table 2(a) shows the assignment of subject threat indices to subject clearance levels. For example, $\widehat{\mathsf{Secret}} = 1$.

- However, from the point of view of objects, we expect the threat to increase as object classification levels increase. For example, the compromise of an object that has a Secret level poses a greater threat than an object that has a Classified level.

  Hence, object threat indexes increase with object classification levels. We write $\overbrace{l}$ to denote an object threat index. Formally, $\overbrace{l} = l - 1$. The second column of Table 2(b) shows the assignment of object threat indexes to object classification levels. For example, $\overbrace{\mathsf{Secret}} = 3$.

Note that since we assume that a set of security levels L is to be assigned to subjects and objects respectively, there can be at most $|L| \times |L|$ combinations of subject-object accesses. In this paper, we assume that $|L| = 5$, hence, there can be at most $5 \times 5 = 25$ combinations of subject-object accesses.

4.1. Object-based threat

A formula that respects the properties of Remark 1 for quantitatively measuring the threat likelihood of granting access to a subject s for an object o, where $sl(s) < ol(o)$, is given below.

$$\texttt{Threat}(s, o) = \begin{cases} \frac{(w \times \overbrace{ol(o)}) + \widehat{sl(s)}}{(|L_S| \times |L_O|) - 1} & \text{if } sl(s) < ol(o), \text{ where } w = |L|, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

The numerator part of the above given formula is intuitive. Since we require that more importance be given to the threat index of objects, we multiply the object threat index with a weight w that equals the cardinality of the set of security levels L used in the system. Thus, we first achieve a "*weighted* object threat index". Then, we add the threat index of the subject to the weighted object threat index.

Essentially, the numerator part of the formula maps all possible accesses by subjects to objects into an interval $[0..(|L_S| \times |L_O|) - 1]$, where a higher value represents a greater

threat. In order to normalize the threat values into an interval [0..1], we divide the value obtained from the numerator by $(|L_S| \times |L_O|) - 1$. The resultant value represents the *object-based* threat likelihood value that respects the properties of Remark 1.

Table 3 shows a two-dimensional array representation of all possible accesses by subjects to objects. Note that an attempt by a subject s to access an object o, such that $sl(s) \geqslant ol(o)$ does not pose a threat. Hence, in Table 3, we assign a threat value of "zero" to all accesses which are either along or below the diagonal of the array.

Each array entry $[i, j]$ includes a value that represents the threat likelihood of a subject s accessing an object o, where $sl(s) = i$ and $ol(o) = j$ that has been calculated by using Formula 3 with weight $w = 5$. Each array entry also includes its "threat rank" (shown next to the threat likelihood value in Sans Serif font within parenthesis) relative to other accesses, where a higher rank means higher threat.

It can be seen from the threat values of any row in Table 3, which were calculated by using Formula 3, that threat measures increase as object classification levels increase. Note also that, for any particular object classification level, (within each column) threat values increase as subject clearance levels decrease. Specifically, lower threat values are observed for objects with Restricted classification level, whereas higher threats are observed for objects with Top Secret classification level. In particular, the highest threat is observed for subjects with Unclassified clearance while attempting to access objects with `Top Secret` classification level.

4.2. Subject-based threat

As before, we need to devise a formula that respects the properties of Remark 2 to be able to quantitatively measure the threat of granting access to a subject s for an object o, where $sl(s) < ol(o)$. We propose one such formula below and describe its construction.

$$\texttt{Threat}(s, o) = \begin{cases} \frac{(w \times \widehat{sl(s)}) + \overbrace{ol(o)}}{(|L_S| \times |L_O|) - 1} & \text{if } sl(s) < ol(o), \text{ where } w = |L|, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

In this approach, since we require that more importance be given to the threat index of subjects, we multiply the subject threat index with a weight w that equals the cardinality of the set of security levels L. Thus, we first achieve a "*weighted* subject threat index". Then, we add the threat index of the object to the weighted subject threat index.

Similar to Formula 3, the numerator part of Formula 4 also maps all possible accesses by subjects to objects into an interval $[0..(|L_S| \times |L_O|) - 1]$, where a higher value represents a greater threat. In order to normalize the threat values into an interval [0..1], we divide the value obtained from the numerator by $(|L_S| \times |L_O|) - 1$. The resultant value represents the *subject-based* threat likelihood value that is consistent with Remark 2.

Table 4 shows a two-dimensional array representation of all possible accesses by subjects to objects. As before, we assigned a threat value of "zero" to all accesses where $sl(s) \geqslant ol(o)$ in Table 4 since such accesses does not pose a threat.

Each array entry $[i, j]$ includes a value that represents the threat likelihood of a subject s accessing an object o, where $sl(s) = i$ and $ol(o) = j$. This value has been calculated

by using Formula 4 with weight $w = 5$. Each array entry also includes its "threat rank" (shown next to the threat likelihood value in Sans Serif font within parenthesis) relative to other accesses, where a higher rank means higher threat.

We can see from the threat values of columns in Table 4, which were calculated by using Formula 4, that threat values increase as subject clearance levels decrease. Note also that, for any particular subject clearance level, (within each row) threat values increase as object classification levels increase. Specifically, least threat is observed when subjects who hold a `Secret` clearance attempt to access objects with a `Top Secret` classification. Whereas, higher threats are observed for subjects who hold a `Unclassified` clearance while attempting to access objects with higher classification levels. In particular, highest threat is observed for subjects who hold a `Unclassified` clearance attempting to access objects with a `Top Secret` classification.

4.3. Difference of scores-based threat

4.3.1. Difference weighted by object classification level

As before, we need to devise a formula to be able to quantitatively measure the threat of subject-object accesses that is based on Remark 3, We note that there can be many formulae which satisfy the properties of Remark 3. We give one such formula below and describe its construction.

$$\texttt{Threat}(s,o) = \begin{cases} \frac{(w \times [ol(o) - sl(s)]) + \overbrace{ol(o)}}{(|L_S| \times |L_O|) - 1} & \text{if } sl(s) < ol(o), \text{ where } w = |L|, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Here we need to compute the difference between the security level of objects and subjects. Hence, we first compute $ol(o) - sl(s)$.

Since we require that more importance be given to the difference between object classification level and subject clearance level, in Formula 5, we multiply $ol(o) - sl(s)$ with a weight w that equals the cardinality of the set of security levels L. Thus, we initially achieve a threat index for the difference between the security indexes of objects and subjects. Then, we add the threat index of the object to the initial threat index.

Similar to Formulae 3 and 4, in order to normalize the threat values into an interval [0..1], we divide the value obtained from the numerator by $(|L_S| \times |L_O|) - 1$. The resultant value represents the threat likelihood value that gives more importance to the difference between object classification level and subject clearance level; and also considers object classification levels. Hence, Formula 5 is consistent with properties of Remark 3.

Table 5 shows a two-dimensional array representation of all possible accesses by subjects to objects. As before, we assigned a threat value of "zero" to all accesses where $sl(s) \geqslant ol(o)$ in Table 5 since such accesses do not pose a threat. As before, a "threat rank" is shown next to the threat likelihood value in Sans Serif font in parenthesis within each array entry, where a higher rank means higher threat.

We can see in Table 5 that threat values always increase as the difference between object classification level and subject clearance level increases. Furthermore, whenever such a difference is the same, threat values increase as object classification level increases.

4.3.2. Difference weighted by subject clearance level

As before, we devise a formula to be able to quantitatively measure the threat of subject-object accesses that is based on Remark 4, We note that there can be many formulae which satisfy the properties of Remark 4. We give one such formula below and describe its construction.

$$\texttt{Threat}(s,o) = \begin{cases} \frac{(w \times [ol(o) - sl(s)]) + \widehat{sl(s)}}{(|L_S| \times |L_O|) - 1} & \text{if } sl(s) < ol(o), \text{ where } w = |L|, \text{ and} \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Similar to Formula 5 we firstly need to compute the difference between object classification level and subject clearance level. Hence, we first compute $ol(o) - sl(s)$.

Similar to Formula 5, since we require that more importance be given to the difference between object classification levels and subject clearance levels, we multiply $ol(o) - sl(s)$ by a weight w that at least equals the cardinality of the set of security levels L used in the system. Then, we add the threat index of the subject to the initial threat index.

Similar to Formulae 3, 4 and 5, in order to normalize the threat values into an interval [0..1], we divide the value obtained from the numerator part of Formula 6 by $(|L_S| \times |L_O|) - 1$. The resultant value represents the threat likelihood value that gives more importance to the difference between object classification level and subject clearance level; and also considers subject clearance levels. Hence, Formula 6 is consistent with properties of Remark 4.

Table 6 shows a two-dimensional array representation of all possible accesses by subjects to objects. As before, we assign a threat value of "zero" to all accesses where $sl(s) \geqslant ol(o)$ in Table 6 since such accesses do not pose a threat. As before, a "threat rank" is shown next to the threat likelihood value in Sans Serif font in parenthesis within each array entry, where a higher rank means higher threat.

Similar to Table 5, we can see in Table 6 that threat values always increase as the difference between object classification level and subject clearance level increases. However, unlike Table 5, whenever such a difference is the same, threat values in Table 6 increase as subject clearance levels decrease.

5. Application to the NIST SP 800-30 Risk Assessment Methodology

In the previous section, we have proposed a method for computing the threat of a subject being able to access a given object, denoted by $\texttt{Threat}(s,o)$, within each of the four approaches of our framework. The NIST SP 800-30 standard suggests that impact values of any compromise of security objectives of objects can be obtained from data classification profiles.

In the remainder of this section, we firstly describe data classification policies and the computation of $\texttt{Impact}(o, a)$ by using data classification policies in Section 5.1. Essentially, $\texttt{Impact}(o, a)$ gives the impact value of executing an action $a \in A$ on an object $o \in O$. Recall from Formula 2 that such impact values will be used, together with $\texttt{Threat}(s, o)$, to compute risk scores. Subsequently, in Section 5.2, we demonstrate the application of our threat assessment framework to compute risk scores by using Formula 2. Section 5.3 describes the application of other three threat assessment approaches for computing risk scores.

5.1. Preliminaries

5.1.1. A model for data classification

All information has value. *Data classification* is the task of evaluating the importance of information to ensure that the information receives an appropriate level of protection. The principal objective of the data classification activity is to group an organization's data by varying levels of sensitivity with respect to the security objectives of *confidentiality*, *integrity* and *availability*.

The US Federal Information Processing Standard (FIPS) 199 [10] and NIST Special Publication (SP) 800-60 [11] publications state that the classification of data with respect to the security objectives is *the first step* in developing a risk management framework. Table 7 shows an example of security classification of data based on the US FIPS 199 [10] and NIST SP-800-60 [11] publications, which suggest that information be classified:

- with respect to the objectives of *confidentiality*, *integrity* and *availability*, and
- by using impact values (or sensitivity levels), such as `Low`, `Moderate` and `High`.

Note that no impact values have been defined for the security objectives of object o_1 in Table 7. Hence, we may understand o_1 in Table 7 as an unprotected object and envisage that o_1 has an Unclassified classification level.

Typically, any assignment of impact values to security objectives with respect to a given object will be specified by the policy makers or business owners or data owners within an organization. Furthermore, any such assignment of impact values to security objectives of objects will sufficiently represent the damage or loss caused to the organization (or its business processes) should the security objectives be compromised.

The definition of impact values $\{\texttt{Low}, \texttt{Moderate}, \texttt{High}\}$ is quoted below as stated in the US FIPS 199 [10] and NIST SP-800-60 [11] publications.

- "The potential impact is `Low` if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals".
- "The potential impact is `Moderate` if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals."

- "The potential impact is `High` if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals."

In practice, any such security classification of data will typically be made within the context of an organization that owns the data, and may be based on the inputs provided by the domain or security experts within that organization.

Essentially, a security classification profile for data stresses the importance of the required protection levels for the data. For example,

- In a financial services scenario, such as electronic payment systems, it is often the case that the confidentiality of credit card numbers has more significance than the availability of such data for processing payments. Hence, the protection levels for the confidentiality objective of data representing credit card information could be high, whereas the protection levels for the availability objective of such information may comparatively be less important.

- However, in a medical services scenario, such as health insurance companies, is often required that data representing the health information of individuals must be highly confidential, must be prevented from inappropriate or unauthorized modifications and must be available when required. Hence, the protection levels for all the three security objectives (confidentiality, integrity and availability) of such data may have equal importance.

- We may envisage a third scenario where the data may be publicly known information, but is used for mission-critical and high-availability systems. In such scenarios, the protection for the confidentiality objective of such data need not be addressed at all, whereas the protection levels for the integrity and availability objectives of such data could be of significance.

Security classification of data is widely practised in the real-world, and is not merely a theoretical concept. For example,

- The Information Security Office, Stanford University, USA has authored *Data Classification Guidelines* for securing the data that is stored within its information systems [12].

- The Government of Alberta, Canada has developed an *Information Security Classification Guideline* to assist its ministries in establishing effective security classification practices for the information that is stored or maintained by them [13].

We now formalize the assignment of impact values to the security objectives of objects. Let $SO = \{\texttt{confidentiality}, \texttt{integrity}, \texttt{availability}\}$ denote the set of security objectives. We admit the existence of a set of impact values $IV = \{\texttt{Low}, \texttt{Moderate}, \texttt{High}\}$ that can be assigned to security objectives for objects. Specifically, every object $o \in O$ is

associated with the set of security objectives SO. We then assign an impact value $iv \in IV$ for every object $o \in O$ with respect to each security objective $so \in SO$. A function $Impact : O \times SO \rightarrow IV$ represents the assignment of impact levels to objects for each security objective $sc \in SO$.

5.1.2. Observations

We now make a few simple observations about the effect of actions on security objectives. These observations have long been known and are intuitive. In order to facilitate our understanding, it is necessary to precisely define the set of actions that we consider. Specifically, we consider "standard" actions such as $A = \{$`read, write, delete`$\}$.

We assume that every action $a \in A$ specifies a single operation and is *atomic*. In particular, action `read` allows *only* the viewing of existing data, action `write` allows *only* the creation of new data, and action `delete` allows *only* the destruction of existing data. It is possible to combine two or more atomic actions for creating a *composite* action. For example, we can create a composite action `modify` that allows both creation of new data and destruction of existing data. However, in this paper, we *only* consider atomic actions. We then note the following:

- action `read` has an effect on `confidentiality` security objective,
- action `write` has an effect on `integrity` security objective,
- action `delete` has an effect on `availability` security objective.

We define a function $sec\_obj : A \rightarrow SO$ that specifies a relationship between each action $a \in A$ and security objectives $so \in SO$.

The above assumptions can easily be extended for considering "composite" access rights that include two or more standard access rights. For example, we may regard `update/modify` as a composite access right that includes the following two standard access rights: {`read, write, delete`}. Such a composite access right may have an effect on two or more security objectives; in this case, we need to define the function sec_obj as $A \rightarrow 2^{SO}$.

Note that `read` and `write` operations may also affect the availability criterion; this can happen as a consequence of a *slow read attack*, for example. However, such attacks, and denial of service (DoS) attacks, can only be analyzed by taking into consideration the fact that operations take time, leading to a server overloads. Timing considerations open a completely new dimension, that we could not include in this paper. Furthermore, the goal of DoS attacks is not to gain unauthorized access to systems or its data, but to restrict legitimate subjects from gaining access to system resources. The scope of this paper is to assess the risk of requests which are initiated by legitimate subjects within the organization to access resources for which they may not be pre-authorized. Hence, consideration of DoS attack parameters is outside the scope of this paper.

5.1.3. Determining impact level of permissions

We model *permissions* as a set $P \subseteq O \times A$. A permission $(o, a) \in P$ specifies that action $a \in A$ can be performed on an object $o \in O$. As noted in Section 5.1.2, there exists a one-to-one mapping between the set of standard access rights $\{\texttt{read}, \texttt{write}, \texttt{delete}\}$ and the set of security objectives $\{\texttt{confidentiality}, \texttt{integrity}, \texttt{availability}\}$. Hence, we could derive the impact level of a given permission $p = (o, a)$ by using functions $sec\_obj : A \rightarrow SO$ and $Impact : O \times SO \rightarrow IV$.

Specifically, we first derive the security objective $so \in SO$ that corresponds to access right a by using function sec_obj. Then, we use $so = sec\_obj(a)$ as one of the input parameters of function $Impact$ for determining the level that object o has with respect to security objective so.

In summary, the impact level of a permission $p = (o, a)$ is given by $Impact(o, sec\_obj(a))$. In the rest of the paper, we write $pl(o, a)$ as a shorthand for $Impact(o, sec\_obj(a))$.

Consider, for example, object o_2 whose data classification is shown in Table 7. Suppose that there exist two permissions $p = (o_2, read)$ and $p' = (o_2, write)$. If we were to determine the impact level of these two permissions, then, according to Table 7, the level of permissions p and p' are determined as follows:

- $pl(p) = Impact(o_2, sec\_obj(\texttt{read})) = Impact(o_2, \texttt{confidentiality}) = \texttt{Low}$.
- $pl(p') = Impact(o_2, sec\_obj(\texttt{write})) = Impact(o_2, \texttt{integrity}) = \texttt{High}$.

5.2. Object-based risk assessment

Table 8 shows the risk scores by using object-based threat likelihood values and impact values. Such threat values are obtained by using Formula 2. In this table, rows are indexed with subject clearance levels and columns are indexed with objects and their classification levels. Furthermore, for each of the objects $\{o_2, o_3, o_4, o_5\}$ shown in Table 8, the subjective impact levels of `confidentiality`, `integrity` and `availability` objectives are borrowed from the data classification profile shown in Table 7.

In order to be able to quantify risk scores, it is necessary to assign a value for each subjective impact level $\{\texttt{Low}, \texttt{Moderate}, \texttt{High}\}$. Generally, such an assignment of values to subjective impact levels is at the discretion of organizations, and may vary from one organization to another. However, for the purposes of demonstration (similar to the NIST SP 800-30 standard) we chose to assign values to subjective impact levels in Table 8 as follows: $\texttt{Low} = 10, \texttt{Moderate} = 50, \texttt{High} = 100$.

Recall that, in Table 7, no impact values have been defined for the security objectives of object o_1, since o_1 is an unprotected object that has a security level Unclassified. Since the computation of risk scores for unprotected objects is not necessary, we do not include object o_1 of Table 7 in Table 8.

Each entry of the table shows the risk score obtained by using Formula 2. We now describe the computation of risk scores shown in Table 8. Consider, for example, a subject $s_1 \in S$ where $sl(s_1) = \text{Unclassified}$ and object o_2 in Table 8, where $ol(o_2) = \text{Restricted}$.

Assume that subject s_1 initiates a request to perform action $read$ on object o_2. Then, the risk score of $(s_1, o_2, read)$ is computed as follows:

- $\texttt{Threat}(s_1, o_2) = 0.38$ (obtained from Table 3 that shows object-based threat measures),
- $\texttt{Impact}(o_2, read) = \texttt{Impact}(o_2, sec\_obj(read)) = \texttt{Impact}(o_2, \texttt{confidentiality}) = 10$,
- $\texttt{Risk}(s_1, o_2, read) = \texttt{Threat}(s_1, o_2) \times \texttt{Impact}(o_2, read) = 0.38 \times 10 = 3.8$.

Assume now that subject s_1 initiates a request to perform action *write* on object o_2. Recall that action *write* has an effect on `integrity` objective. Then, it can be seen from Table 8 that $\texttt{Risk}(s_1, o_2, write)$ is 19.

It can be seen from the above two scenarios that: since the same subject is accessing the same object in both scenarios, the threat likelihood values remain the same. However, executing action *write* on o_2 (that has an effect on the `integrity` objective) has a higher impact value than executing action *read* on o_2 (that has an effect on the `confidentiality` objective). Hence, Scenario 2 has a higher risk score than Scenario 1. We therefore say that our risk scores capture both threat likelihood values and impact values.

Now let us consider, for example, subject s_1 from the above two scenarios and object o_3 in Table 8, where $ol(o_3) = \mathsf{Classified}$. Assume that subject s_1 initiates a request to perform action *write* on object o_3. Then, we can see in Table 8 that $\texttt{Risk}(s_1, o_3, write)$ is 29.

We can observe from Scenarios 2 and 3 that: although the impact values remain the same in both scenarios, Scenario 3 has a higher risk score than Scenario 2. This is because the threat likelihood value of subject s_1 accessing object o_2 is greater than s_1 accessing o_3. Thus, we can see that risk scores increase as object levels increase.

Now let us consider, for example, another subject s_2, where $sl(s_2) = \mathsf{Restricted}$ and object o_3 in Table 8, where $(o_3) = \mathsf{Classified}$. Assume that subject s_2 initiates a request to perform action *write* on object o_3. Then, it can be seen from Table 8 that $\texttt{Risk}(s_2, o_3, write)$ is 27.

We can observe from the above two scenarios that: although the impact values remain the same in both scenarios, $(s_1, o_3, write)$ has a higher risk score than $(s_2, o_3, write)$. This is because the threat likelihood value of subject s_1 accessing object o_3 is greater than s_2 accessing o_3. Thus, we can see that: whenever object levels and impact values remain the same, risk scores increase as subject levels decrease.

5.3. Applying other threat assessment approaches for risk assessment

In this section, we describe the computation of risk scores by using subject-based threat assessment (see Table 9) and difference of security levels based threat assessment (see Tables 10 and 11).

For the purposes of consistency with Table 8, the rows and columns of Tables 9, 10 and 11 are indexed with subject clearance levels and objects classification levels, respectively. Furthermore, similar to Table 8, for each of the objects $\{o_2, o_3, o_4, o_5\}$ shown in Tables 9, 10 and 11, the subjective impact levels of `confidentiality`, `integrity` and `availability` objectives is borrowed from the data classification profile shown in Table 7.

As in Table 9, we assigned values to subjective impact levels in Tables 9, 10 and 11, as follows: $\texttt{Low} = 10, \texttt{Moderate} = 50, \texttt{High} = 100$. As before, we chose not to include object o_1 of Table 7 in Tables 9, 10 and 11 because no impact levels have been specified for the security objectives of o_1.

Table 9 shows risk scores where threat likelihood values are subject-based and obtained by using Formula 2. Each entry of Table 9 shows the risk score obtained by using Formula 2.

Table 10 shows risk scores where threat likelihood values are based on the difference between the security level of object and subject. Such threat values are obtained by using Formula 5. Each entry of Table 10 shows the risk score obtained by using Formula 2.

Table 11 shows risk scores where threat likelihood values which are based on the difference between the security level of object and subject and weighted by subject level. Such threat values are obtained by using Formula 6. Each entry of Table 11 shows the risk score obtained by using Formula 2.

6. Proof of Correctness

This section shows that the formulae for threat assessment proposed in Section 4 satisfy properties A and B described in Section 2.

Lemma 1. *Formulae 3, 4, 5 and 6 satisfy properties A and B.*

Proof. We have the following from Formula 3.

$$\texttt{Threat}(s,o) = \begin{cases} \frac{(w \times \overbrace{ol(o)}) + \widehat{sl(s)}}{(|L_S| \times |L_O|) - 1} & \text{if } sl(s) < ol(o), \text{ where } w = |L|, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Suppose that $|L_s|$ and $|L_o|$ are fixed and that $w = |L|$. Then, we have the following.

- When $ol(o)$ increases (or decreases), $\overbrace{(ol(o))} = ol(o) - 1$ also increases (or decreases respectively). Consequently, for any given subject, $Threat(s, o)$ increases (or decreases) as $ol(o)$ increases (or decreases respectively). We deduce that the Formula 3 satisfies property A.

- When $sl(s)$ increases (or decreases), $\widehat{(sl(s))} = w - sl(s)$ decreases (or increases respectively). Consequently, for any given object, $Threat(s, o)$ decreases (or increases) as $sl(s)$ increases (or decreases respectively). We deduce that Formula 3 satisfies property B.

□

Proofs for Formulae 4, 5 and 6 are similar.

7. Discussion

7.1. Related Work

The ISO/IEC 27005:2011 standard [14] provides guidelines for information security risk management in an organization. The ISO/IEC 27005:2011 standard suggests that:

- threats may be of natural or human origin and may arise from within or outside the organization.
- impact criteria should consider breaches of information security, for example, loss of confidentiality, integrity and availability.
- risk values can be derived as a product of threat and impact values.

Note that the scope of proposed framework is only to consider threats in terms of unauthorized access requests initiated by subjects (human users) within the organization. This means that the proposed framework is narrow in scope and is only able to consider a subset of threats that could potentially occur in a real world. Similar to this standard, our framework computes impact values based on the loss of confidentiality, integrity and availability of data objects. We believe that our framework that computes risk scores as a product of threat and impact values, conforms to the high-level risk assessment approach of ISO/IEC 27005:2011. It should be noted that this standard does not provide any specific method for information security risk assessment. In contrast, our framework provides specific methods for risk assessment that is based on four different threat assessment approaches: each suited to a specific situation based on organizations' point of view.

Cheng *et al* proposed Fuzzy Multi-Level Security (Fuzzy MLS): a method to enforce quantified risk adaptive access control in multi-level security systems [1]. This work quantifies the risk of an access request based on the difference between a subject security level and an object security level. Specifically, in Fuzzy MLS, risk increases as the difference between the security levels of objects and subjects increases. Note that one of the four approaches of our threat assessment framework that is described in Section 4.3 primarily considers the difference between the security levels of permissions and subjects. Hence, computation of risk scores by using Formula 5 of our work produces risk scores which intuitively are similar to the Fuzzy MLS approach.

However, our threat assessment framework also includes three other ways to quantify threat likelihood values based on different combinations of intuitive principles, as opposed to a single notion of threat likelihood (that is called as probability of damage) in Fuzzy MLS. Hence, we see our work to be more comprehensive than Fuzzy MLS. Also, while Fuzzy MLS assumes that impact values can be obtained by considering the security levels of objects, our framework uses impact values defined within data classification policies.

Ni *et al* used fuzzy inference techniques as an approach for estimating access risks and to develop an enforcement mechanism for risk based access control [5]. However, access risk is this work is primarily computed by the object security level and secondly by the subject security level. The object-based threat assessment approach that we described in

Section 3.4 considers similar criteria. Hence, we may observe intuitive similarities between the access risk computed in [5] and our object-based threat assessment approach.

However, there exist differences between the work of Ni *et al* [5] and our work. In particular, the work of Ni *et al* uses fuzzy inference techniques to compute risk. In comparison, our work exploits the risk function of NIST SP 800-30 for quantifying access risk within our work as a product of threat likelihood values, which are computed by using the proposed threat assessment formulae, and impact values, which are derived from data classification policies.

Recently, Chari *et al* [15] presented a system, in the context of role-based access control systems (RBAC), that is a practical realization of a fuzzy logic risk inferencing system proposed by Ni *et al*. The work of Chari *et al* estimates risk by referring to the security level of permissions and clearance levels of subjects (referred to as "aggregate user access risk level"). Chen *et al* examined a number of possible ways to define risk in different components of the RBAC model [16]. In particular, they considered the risk of granting a request in the RBAC model in terms of competence and distance between users, roles and permissions. In comparison with [15] and [16], our framework estimates access risk directly between subjects and permissions. We believe that our framework can be extended to consider access risks within RBAC systems and will address risk estimation within RBAC systems as part of our ongoing work. Furthermore, our framework estimates access risk as a product of threat and impact scores, which is similar to the NIST SP 800-30 and ISO/IEC 27005:2011 standards.

Molloy *et al* presented a new learning and risk-based architecture for a local PDP, where a decision is first proposed with a known level of uncertainty [17]. The tradeoff of the uncertainty and utility associated with this decision is then assessed, determining whether the decision can be taken locally or the central PDP should be contacted. They defined three different risk methodologies, namely Expected Utility, Risk Adjusted Utility, and Independent Risk Constraints, each representing a different risk perspective. The main contribution of [17] is to show that machine-learning can be used to make security decisions and to validate the intuitive assumption that the uncertainty of a classifier can be used as an accurate measure of risk. Our framework, which estimates risk as a product of threat and impact scores, is more closer to the widely accepted risk assessment function of NIST SP-800-30.

Bartsch proposed a policy override calculus for qualitative risk assessment in the context of role-based access control systems [9]. In comparison with the work of Bartsch, our work provides support for both qualitative and quantitative threat assessment. We then used quantified threat values to compute risk scores for authorizations of subjects that already exist in the system or for evaluating access requests initiated by subjects. Also, our work quantifies the risk of $(subject, object, action)$ tuples. We believe that our work can easily be extended to quantify risk in the context of role-based systems, and such extensions would be investigated as part of our immediate future work.

Diep *et al* described an access control model with context-based decisions that includes quantitative risk assessment [2]. However, there is little or no description for computing threat likelihood values in [2]. Our framework explicitly describes multiple ways to compute

threat likelihood values, and quantifies access risk as a product of threat likelihood values and impact values.

The novelty of proposed framework is to demonstrate that risk estimates for access requests differ based on the threat assessment approach that has been chosen. To the best of our knowledge, none of the existing risk assessment methods provide this insight.

7.2. Limitations

Note that threat assessment methods in the proposed framework are based on a priori classification of subjects and objects. This means that the proposed framework cannot cover unexpected threats such as insider threats in which several other socio-technical parameters must be taken into consideration for reflecting the reality of internal and external threats such as users' access history, behavior, collusion with other users, etc. Hence, insider threat assessment is outside of the scope of this paper. Similarly, threats related to social engineering concerns cannot be assessed by our framework. In future work, we plan to examine the application of the proposed risk assessment framework for assessing threat and impact of insider threats, along the lines suggested in [18], and social engineering threats.

Furthermore, as stated earlier in Section 5.1.2, certain DoS attacks might compromise the availability criterion by `read` and `write` operations. The proposed framework cannot assess such threats. Adapting the proposed framework for assessing DoS threats would be a subject of our future work.

8. Conclusions

The main contribution of this paper is a framework that includes a family of threat assessment approaches for subject-object accesses, which can be selected based on the context of applications or on the preference of organizations. Specifically, our framework includes four different ways of assessing the threat of subject-object accesses. Our first threat assessment approach, described in Section 3.4, primarily considers the sensitivity scores of objects, and thus gives more priority to the sensitivity of data. We have described another threat assessment approach in Section 3.5 that mainly considers trustworthiness scores of subjects, and thus gives more priority to subject trustworthiness than object sensitivity. A third approach that is based on the idea that threat can be calculated as the difference between object sensitivity and subject trustworthiness scores has been described in Section 4.3, and for this approach we have identified two different subcases by considering the object sensitivity scores and subject trustworthiness scores as secondary parameters.

We have demonstrated that the order in which the "three general threat principles" are applied makes a difference in the resulting threat vectors. This result is important because the approach adopted to assess the threat posed by subjects towards objects will subsequently affect the computation of risk metrics.

To the best of our knowledge, our work represents the first attempt in the literature to conduct a comprehensive study of several alternative approaches for threat assessment

by considering object sensitivity and subject trustworthiness scores. We have presented several examples which justify our threat assessment approaches in intuitive terms. We also proposed formulae to estimate threats that subjects may pose towards data objects.

We then demonstrated the application of our threat assessment framework to estimate risk of access requests by adopting the well accepted risk assessment function of the NIST SP 800-30. Firstly, in order to compute impact values of object-action pairs, we exploited "data classification policies" [11]. Subsequently, we used such impact values together with threat values, which are derived from Formulae 3, 4, 5 and 6, for quantifying risk of $(subject, object, action)$ triples based on Formula 2.

Risk estimates for access requests obtained by using our threat assessment framework are shown in Tables 8, 9, 10 and 11. The main result to note here is that risk estimates for access requests differ based on the threat assessment approach that has been chosen. Therefore, organizations must make prudent judgement while selecting a risk assessment function for risk-based access control systems.

To the best of our knowledge, our work also represents the first attempt in the literature to develop, and compare, different approaches for estimating the risk of access requests (unlike [1, 5]).

There exist opportunities for extending the work presented in this paper. As mentioned earlier, opportunities for future work include consideration of risk assessment within the context of RBAC systems and assess threats by considering DoS parameters. Another future direction would be to extend and refine the quantification methods for threat assessment that we have proposed in many ways. We proposed formulae for quantifying threat values and numerically evaluated those formulae within each of the four approaches that we have proposed. Different looking formulae could be invented which could lead to equivalent results. Developing a theory for the study of the properties and application of such formulae could be a subject for future research.

Acknowledgment

We gratefully acknowledge the inputs of reviewers whose constructive suggestions have been instrumental for improving preliminary drafts of this paper. The work presented in paper was funded in part by grants of the Natural Sciences and Engineering Research Council of Canada and CA Technologies. We thank Serge Mankovski for having provided the initial motivation for this research.

References

[1] P.-C. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, A. Reninger, Fuzzy multilevel security: An experiment on quantified risk-adaptive access control, in: Proceedings of IEEE Symposium on Security and Privacy, (SP '07), 2007, pp. 222 –230.

[2] N. N. Diep, L. X. Hung, Y. Zhung, S. Lee, Y.-K. Lee, H. Lee, Enforcing access control using risk assessment, in: Proceedings of the 4th European Conference on Universal Multiservice Networks (ECUMN'07), 2007, pp. 419–424.

[3] S. Kandala, R. Sandhu, V. Bhamidipati, An attribute based framework for risk-adaptive access control models, in: Proceedings the 6th International Conference on Availability, Reliability and Security (ARES'11), 2011.

[4] R. McGraw, Risk adaptive access control (RAdAC), in: Proceedings of NIST & NSA Privilege Management Workshop, 2009.

[5] Q. Ni, E. Bertino, J. Lobo, Risk-based access control systems built on fuzzy inferences, in: Proceedings of 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS'10), 2010, pp. 250–260.

[6] Q. Wang, H. Jin, Quantified risk-adaptive access control for patient privacy protection in health information systems, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11), 2011, pp. 406–410.

[7] NIST, Risk management guide for information technology systems, National Institute of Standards and Technology, Special Publication (SP) 800-30 (2002).

[8] NIST, Guide for conducting risk assessments, National Institute of Standards and Technology, Special Publication (SP) 800-30 Revison 1 (2012).

[9] S. Bartsch, A calculus for the qualitative risk assessment of policy override authorization, in: Proceedings of the 3rd International Conference on Security of Information and Networks (SIN'10), 2010, pp. 62–70.

[10] NIST, Standards for security categorization of federal information and information systems, Federal Information Processing Standards Publication, FIPS Publication 199 (2004).

[11] NIST, Guide for mapping types of information and information systems to security categories, National Institute of Standards and Technology, Special Publication (SP) 800-60, volumes I & II (2008).

[12] Stanford University - Information Security Office, Stanford data classification guidelines, available at `http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html`.

[13] The Government of Alberta, Canada, Information security classification, available at `https://www.rimp.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf` (2005).

[14] ISO/IEC, Information technology – Security techniques – Information security risk management, International Standard, Reference number ISO/IEC 27005:2011(E) (June 2011).

[15] S. Chari, J. Lobo, I. Molloy, Practical risk aggregation in rbac models, in: Proceedings of the 17th ACM symposium on Access Control Models and Technologies, SACMAT '12, 2012, pp. 117–118.

[16] L. Chen, J. Crampton, Risk-aware role-based access control, in: Proceedings of 7th International Workshop on Security and Trust Management, Vol. 7170 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2012, pp. 140–156.

[17] I. Molloy, L. Dickens, C. Morisset, P.-C. Cheng, J. Lobo, A. Russo, Risk-based security decisions under uncertainty, in: Proceedings of the second ACM conference on Data and Application Security and Privacy (CODASPY'12), 2012, pp. 157–168.

[18] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. J. Shimeall, L. Flynn, Common sense guide to mitigating insider threats - 4th edition, Tech. rep., Software Engineering Institute, Carnegie Mellon University, Availale at `http://www.sei.cmu.edu/reports/12tr012.pdf` (December 2012).

Table 1: Configuration of the running example

(a) Subjects and trustworthiness scores

Subject	**Trustworthiness Score**
`Alice`	90
`Bob`	80
`Carol`	70
`Dave`	80

(b) Objects and sensitivity scores

Object	**Sensitivity Score**	**Object Description**
o	90	`location` of weapons
o'	100	`launch codes` of weapons

Table 2: Threat indices

(a) Subject threat indices

Subject Security Level	**Subject Threat Index**
Unclassified: 1	4
Restricted: 2	3
Classified: 3	2
Secret: 4	1
Top Secret: 5	0

(b) Object threat indices

Object Security Level	**Object Threat Index**
Unclassified: 1	0
Restricted: 2	1
Classified: 3	2
Secret: 4	3
Top Secret:5	4

Table 3: Object-based threat likelihood values by using Formula 3

Subject Clearance Levels	**Object Classification Levels**				
	Unclassified : 1	**Restricted : 2**	**Classified : 3**	**Secret : 4**	**Top Secret : 5**
Unclassified : 1	0	0.38 (1)	0.58 (3)	0.79 (6)	1.0 (10)
Restricted : 2	0	0	0.54 (2)	0.75 (5)	0.96 (9)
Classified : 3	0	0	0	0.71 (4)	0.92 (8)
Secret : 4	0	0	0	0	0.88 (7)
Top Secret : 5	0	0	0	0	0

Table 4: Subject-based threat likelihood values by using Formula 4

Subject Clearance Levels	**Object Classification Levels**				
	Unclassified : 1	**Restricted : 2**	**Classified : 3**	**Secret : 4**	**Top Secret : 5**
Unclassified : 1	0	0.88 (7)	0.92 (8)	0.96 (9)	1.0 (10)
Restricted : 2	0	0	0.71 (4)	0.75 (5)	0.79 (6)
Classified : 3	0	0	0	0.54 (2)	0.58 (3)
Secret : 4	0	0	0	0	0.38 (1)
Top Secret : 5	0	0	0	0	0

Table 5: *Difference of security levels*-based threat likelihood values weighted with object level obtained by using Formula 5

Subject Clearance Levels	**Object Classification Levels**				
	Unclassified : 1	**Restricted : 2**	**Classified : 3**	**Secret : 4**	**Top Secret : 5**
Unclassified : 1	0	0.25 (1)	0.50 (5)	0.75 (8)	1.0 (10)
Restricted : 2	0	0	0.29 (2)	0.54 (6)	0.79 (9)
Classified : 3	0	0	0	0.33 (3)	0.58 (7)
Secret : 4	0	0	0	0	0.37 (4)
Top Secret : 5	0	0	0	0	0

Table 6: *Difference of security levels*-based threat likelihood values weighted with subject level obtained by using Formula 6

Subject Clearance Levels	**Object Classification Levels**				
	Unclassified : 1	**Restricted : 2**	**Classified : 3**	**Secret : 4**	**Top Secret : 5**
Unclassified : 1	0	0.37 (4)	0.58 (7)	0.79 (9)	1.0 (10)
Restricted : 2	0	0	0.33 (3)	0.54 (6)	0.75 (8)
Classified : 3	0	0	0	0.29 (2)	0.50 (5)
Secret : 4	0	0	0	0	0.25 (1)
Top Secret : 5	0	0	0	0	0

Table 7: Data classification profile based on the US FIPS 199 [10] and NIST SP-800-60 [11] publications

Objects	**Confidentiality**	**Integrity**	**Availability**
o_1	n/a	n/a	n/a
o_2	Low	Moderate	High
o_3	Moderate	Moderate	Moderate
o_4	High	Low	Low
o_5	High	Moderate	High

Table 8: *Object*-based risk scores

Subject Clearance Levels	**Object Classification Levels**											
	o_2: **Restricted**			o_3: **Classified**			o_4: **Secret**			o_5: **Top Secret**		
	con= Low (10)	int= Moderate (50)	ava= High (100)	con= Moderate (50)	int= Moderate (50)	ava= Moderate (50)	con= High (100)	int= Low (10)	ava= Low (10)	con= High (100)	int= Moderate (50)	ava= High (100)
Unclassified	$0.38 \times 10 = 3.8$	$0.38 \times 50 = 19$	$0.38 \times 100 = 38$	$0.58 \times 50 = 29$	$0.58 \times 50 = 29$	$0.58 \times 50 = 29$	$0.79 \times 100 = 79$	$0.79 \times 10 = 7.9$	$0.79 \times 10 = 7.9$	$1.0 \times 100 = 100$	$1.0 \times 50 = 50$	$1.0 \times 100 = 100$
Restricted	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0.54 \times 50 = 27$	$0.54 \times 50 = 27$	$0.54 \times 50 = 27$	$0.75 \times 100 = 75$	$0.75 \times 10 = 7.5$	$0.75 \times 10 = 7.5$	$0.96 \times 100 = 96$	$0.96 \times 50 = 48$	$0.96 \times 100 = 96$
Classified	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0.71 \times 100 = 71$	$0.71 \times 10 = 7.1$	$0.71 \times 10 = 7.1$	$0.92 \times 100 = 92$	$0.92 \times 50 = 46$	$0.92 \times 100 = 92$
Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0.88 \times 100 = 88$	$0.88 \times 50 = 44$	$0.88 \times 100 = 88$
Top Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$

Table 9: *Subject*-based risk scores

Subject Clearance Levels	**Object Classification Levels**											
	o_2: **Restricted**			o_3: **Classified**			o_4: **Secret**			o_5: **Top Secret**		
	con= Low (10)	int= Moderate (50)	ava= High (100)	con= Moderate (50)	int= Moderate (50)	ava= Moderate (50)	con= High (100)	int= Low (10)	ava= Low (10)	con= High (100)	int= Moderate (50)	ava= High (100)
Unclassified	$0.88 \times 10 = 8.8$	$0.88 \times 50 = 44$	$0.88 \times 100 = 88$	$0.92 \times 50 = 46$	$0.92 \times 50 = 46$	$0.92 \times 50 = 46$	$0.96 \times 100 = 96$	$0.96 \times 10 = 9.6$	$0.96 \times 10 = 9.6$	$1.0 \times 100 = 100$	$1.0 \times 50 = 50$	$1.0 \times 100 = 100$
Restricted	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0.71 \times 50 = 35.5$	$0.71 \times 50 = 35.5$	$0.71 \times 50 = 35.5$	$0.75 \times 100 = 75$	$0.75 \times 10 = 7.5$	$0.75 \times 10 = 7.5$	$0.79 \times 100 = 79$	$0.79 \times 50 = 39.5$	$0.79 \times 100 = 79$
Classified	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0.54 \times 100 = 54$	$0.54 \times 10 = 5.4$	$0.54 \times 10 = 5.4$	$0.58 \times 100 = 58$	$0.58 \times 50 = 29$	$0.58 \times 100 = 58$
Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0.38 \times 100 = 38$	$0.38 \times 50 = 19$	$0.38 \times 100 = 38$
Top Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$

Table 10: *Difference of object and subject security levels*-based risk scores Weighted by Object Levels

Subject Clearance Levels	**Object Classification Levels**											
	o_2: **Restricted**			o_3: **Classified**			o_4: **Secret**			o_5: **Top Secret**		
	con= Low (10)	int= Moderate (50)	ava= High (100)	con= Moderate (50)	int= Moderate (50)	ava= Moderate (50)	con= High (100)	int= Low (10)	ava= Low (10)	con= High (100)	int= Moderate (50)	ava= High (100)
Unclassified	$0.25 \times 10 = 2.5$	$0.25 \times 50 = 12.5$	$0.25 \times 100 = 25$	$0.50 \times 50 = 25$	$0.50 \times 50 = 25$	$0.50 \times 50 = 25$	$0.75 \times 100 = 75$	$0.75 \times 10 = 7.5$	$0.75 \times 10 = 7.5$	$1.0 \times 100 = 100$	$1.0 \times 50 = 50$	$1.0 \times 100 = 100$
Restricted	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0.29 \times 50 = 14.5$	$0.29 \times 50 = 14.5$	$0.29 \times 50 = 14.5$	$0.54 \times 100 = 54$	$0.54 \times 10 = 5.4$	$0.54 \times 10 = 5.4$	$0.79 \times 100 = 79$	$0.79 \times 50 = 39.5$	$0.79 \times 100 = 79$
Classified	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0.33 \times 100 = 33$	$0.33 \times 10 = 3.3$	$0.33 \times 10 = 3.3$	$0.58 \times 100 = 58$	$0.58 \times 50 = 29$	$0.58 \times 100 = 58$
Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0.37 \times 100 = 37$	$0.37 \times 50 = 18.5$	$0.37 \times 100 = 37$
Top Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$

Table 11: *Difference of object and subject security levels*-based risk scores Weighted by Subject Levels

Subject Clearance Levels	**Object Classification Levels**											
	o_2: **Restricted**			o_3: **Classified**			o_4: **Secret**			o_5: **Top Secret**		
	con= Low (10)	int= Moderate (50)	ava= High (100)	con= Moderate (50)	int= Moderate (50)	ava= Moderate (50)	con= High (100)	int= Low (10)	ava= Low (10)	con= High (100)	int= Moderate (50)	ava= High (100)
Unclassified	$0.37 \times 10 = 3.7$	$0.37 \times 50 = 18.5$	$0.37 \times 100 = 37$	$0.58 \times 50 = 29$	$0.58 \times 50 = 29$	$0.58 \times 50 = 29$	$0.79 \times 100 = 79$	$0.79 \times 10 = 7.9$	$0.79 \times 10 = 7.9$	$1.0 \times 100 = 100$	$1.0 \times 50 = 50$	$1.0 \times 100 = 100$
Restricted	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0.33 \times 50 = 16.5$	$0.33 \times 50 = 16.5$	$0.33 \times 50 = 16.5$	$0.54 \times 100 = 54$	$0.54 \times 10 = 5.4$	$0.54 \times 10 = 5.4$	$0.75 \times 100 = 75$	$0.75 \times 50 = 37.5$	$0.75 \times 100 = 75$
Classified	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0.29 \times 100 = 29$	$0.29 \times 10 = 2.9$	$0.29 \times 10 = 2.9$	$0.50 \times 100 = 50$	$0.50 \times 50 = 25$	$0.50 \times 100 = 50$
Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0.25 \times 100 = 25$	$0.25 \times 50 = 12.5$	$0.25 \times 100 = 25$
Top Secret	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$	$0 \times 10 = 0$	$0 \times 10 = 0$	$0 \times 100 = 0$	$0 \times 50 = 0$	$0 \times 100 = 0$