A RISK BASED APPROACH FOR SELECTING SERVICES IN BUSINESS PROCESS EXECUTION

Stefan Sackmann
University of Freiburg, Institute of Computer Science & Social Studies, Department of Telematics

Lutz Lowis
University of Freiburg, Institute of Computer Science & Social Studies, Department of Telematics

Kai Kittel
University of Freiburg, Institute of Computer Science & Social Studies, Department of Telematics

Follow this and additional works at: http://aisel.aisnet.org/wi2009

Recommended Citation
http://aisel.aisnet.org/wi2009/38
Abstract
The vision of automated business processes within a service-oriented paradigm includes the flexible orchestration of IT services. Whenever alternative services are available for activities in an IT-supported business process, an automated decision is worth aspiring to. According to value-oriented management, this decision should be motivated economically and also requires taking account of risk. This paper presents a novel approach for assessing the risk of IT services, based on vulnerability information as can be obtained in the form of publicly available Common Vulnerability Scoring System (CVSS) data.

1. Automating IT service selection

Market forces are raising companies’ ability to respond quickly and flexibly to changing demands, which is seen as one of the main competitive advantages of the future [1, 23]. To keep pace, directing business models towards automation is still regarded as an important strategic topic [25] and aligning the technological infrastructure to service oriented architecture (SOA) seems a feasible and promising way [10, 16]. Apparently, present SOA and standards such as BPEL or BPMN are still in need of improvement to satisfy business demands [29] and the present hype around service orientation is endangered by setbacks [13]. Nevertheless, prominent suppliers of hard- and software are already embodying service orientation into their products: IBM offers Websphere [19], SAP integrates Netweaver [6], and Microsoft uses services in Windows Vista [4].

Besides the technical feasibility of SOA, exploiting the full potential of services requires solutions to several business demands. In this contribution, the focus is laid on one of these issues: the automated selection between alternative IT services available for supporting the execution of business process activities. Since the ability of an IT service to meet business process-specific protection goals is crucial, a method for assessing the risk of an IT service within the context of the supported business process is developed. The method consists of two major parts: The first part proposes a new way to measure the probability of achieving protection goals within an IT service by assessing vulnerabilities. The second part extends business process models by an economic decision algorithm that also takes risk into consideration and enables an automated decision between alternative IT services in the concrete execution context. Addressing these two parts, the remainder of this contribution is structured as follows: in section 2, a layer-based model is introduced bringing

---

1 University of Freiburg, Institute of Computer Science & Social Studies, Department of Telematics, Friedrichstrasse 50, 79098 Freiburg, Germany
the economic and technical view of IT risk together and serving as starting point for structuring IT services. Based upon this model, in section 3, a measure for the ability of an IT service to achieve protection goals from IT security research is presented and discussed. In section 4, this measure is integrated into an economic decision algorithm for business process activities taking the riskiness of alternative IT services into consideration. Subsequently, it is demonstrated how the algorithm works by means of an exemplified purchase process. The contribution concludes by discussing limitations of the method and by proposing possible solutions.

2. IT Risk Reference Model - Bridging the technical and economic view

The challenges to a value-oriented risk management process and continuous risk assessment, resulting from a constantly changing IT support of business processes as in SOA, have been discussed in [20, 21]. Following the notion of service orientation, automating business processes means that services are not exclusively used for one specific business process but manifold. Furthermore, the orchestration of the IT services changes dynamically according to the business context and is not statically wired in advance at the time when the business process is designed. Since the economic risk depends on the business process supported, the riskiness of an IT service should be specified independently of its actual integration. Therefore, typical measures for assessing IT security that already include economic exposure, e.g. an annual loss expectancy (ALE) [3] or business adjusted risk (BAR) [12], are unsuitable. It seems more advisable to look for measures that characterize the riskiness of IT services in a form that can be integrated into the service description and thus, e.g., become part of a service or protection level agreement (SLA/PLA) [14]. The approach in hand has been developed with a focus on services provided within a trusted domain, i.e. a company’s internal services or external services of business partners under contractual relationship.

![Figure 1: IT Risk Reference Model [20]](image)

For measuring the riskiness of IT services, the measures used should rely on a systematic modeling of relations between causes and effects of IT risks. For this purpose, the IT Risk Reference Model has been developed [20] that is structured following a hierarchical abstraction layer model as used in computer science for reducing complexity, e.g. in network communication [28]. On the basis of four different layers (Figure 1), the economic, process-oriented view is brought together with the technical, threat-oriented view of IT risk. Beginning with the economic view, the top layer represents the “effects” and contains all activities of the business process that are regarded as assets from a risk perspective. The next layer contains all IT services and their underlying IT infrastructure representing IT resources for the superordinated process activities. Vulnerabilities constitute the “bridge” between the economic and the technical layers since they are possible points of attack for threats violating protection goals of the IT applications [24]. Thus, since a large part of attacks re-
sult from exploitation of known vulnerabilities (see e.g. [22]), the following layer represents the vulnerabilities of these applications, while the set of all known threats is part of the bottom layer representing the causes.

Although the IT Risk Reference Model has been developed with a different focus on measuring changes between causes and effects of IT risk, the achievable link provides a suitable starting point for the aspired measure. Since vulnerabilities can only be identified in relation to protection goals [17], measuring the probabilities of an IT service to achieve protection goals that are relevant to superordinated business processes is seen as a promising approach. In IT security research, there are several protection goals discussed [5, 17, 30]. For the beginning, focusing on the three main protection goals, confidentiality, integrity, and availability (CIA), is proposed for mainly three reasons: firstly, since the riskiness of an IT service is highly dependent on the IT security achieved, these protection goals are relevant for business processes [18]. Secondly, there is a well established methodical understanding of these protection goals in IT security research [2]. Thirdly, focusing on high-level protection goals does not limit the applicability of the method: more context-specific protection goals can be considered. According to this view, an IT service is considered to be secure (no risk) if it has no known vulnerabilities affecting the IT service’s confidentiality, integrity, or availability of data or processes.

A decision-theory based selection requires two measures (Figure 2). Firstly, the damage resulting from non-achievement different protection goals has to be quantified according to the context of the business process. This could be realized either by relative evaluation (see, e.g., the POSeM model of [18]) or monetary assessment, e.g. in the form of expected loss and will be discussed in more detail in section 4. Secondly, it is necessary to determine the probability of an IT service violating the protection goals. For assessing these probabilities automatically, a new method is proposed in the following section.

3. Measuring IT Service Riskiness

Following the IT Risk Reference Model, vulnerabilities are the key factor since they allow attackers to harm protection goals. It is assumed that not all known vulnerabilities can instantly be closed for economical and technical reasons (e.g., limited time and money, patches not available). Otherwise, a risk-based approach would be pointless. Prominent methods for identifying vulnerabilities are penetration tests [2] or source code analysis [7]. Furthermore, for the technical infrastructure on which the IT services run, vulnerabilities can be queried from publicly accessible vulnerability databases. This allows an initial estimation of a company’s security level by looking at the sheer
number of known vulnerabilities, as well as gauging the effects a given vulnerability’s exploitation would have on the individual IT security protection goals.

3.1. Vulnerability Information Sources

The approach presented works with any vulnerability database that offers information on the CIA impact caused through exploiting a given vulnerability. In this contribution, the well known Common Vulnerabilities and Exposures (CVE) [8] database is used offering data according to the Common Vulnerability Scoring System (CVSS) as shown in Table 1. The Base Score Metrics not only indicate the impact of exploiting a vulnerability, but also where it can be exploited from, how complex the exploit is, and how often the attacker must authenticate to the target. The Temporal Score Metrics offer detailed information on the availability of an exploit, existing countermeasures, and the credibility of the vulnerability details.

Table 1: CVE scheme and CVSS values [9]

<table>
<thead>
<tr>
<th>CVSS metric group</th>
<th>CVSS metric</th>
<th>CVSS values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Score Metrics</td>
<td>Access Vector</td>
<td>local (0.395), adjacent network (0.646), network (1)</td>
</tr>
<tr>
<td></td>
<td>Access Complexity</td>
<td>low (0.71), medium (0.61), high (0.35)</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
<td>none (0.704), single (0.56), multiple (0.45)</td>
</tr>
<tr>
<td></td>
<td>Confidentiality Impact</td>
<td>none (0), partial (0.275), complete (0.66)</td>
</tr>
<tr>
<td></td>
<td>Integrity Impact</td>
<td>none (0), partial (0.275), complete (0.66)</td>
</tr>
<tr>
<td></td>
<td>Availability Impact</td>
<td>none (0), partial (0.275), complete (0.66)</td>
</tr>
<tr>
<td>Temporal Score Metrics</td>
<td>Exploitability</td>
<td>unproven (0.85), proof-of-concept (0.9), functional (0.95), high (1), not defined (1)</td>
</tr>
<tr>
<td></td>
<td>Remediation Level</td>
<td>official fix (0.87), temporary fix (0.9), workaround (0.95), unavailable (1), not defined (1)</td>
</tr>
<tr>
<td></td>
<td>Report Confidence</td>
<td>unconfirmed (0.9), uncorroborated (0.95), confirmed (1), not defined (1)</td>
</tr>
</tbody>
</table>

At present, the vast majority of CVE entries relates to software applications other than web services. In future, once a critical amount of web services is in operational use, web service vulnerabilities can be expected to be listed in CVE or a similar database. Therefore, for assessing IT services, exemplary values of actual CVE entries for software applications are used in this contribution.
3.2. CVSS and Attack Probabilities

In practice, attack probabilities often rely on subjective expert estimates given by, e.g., system administrators with a varying degree of experience, which is seen as a major drawback in the IT security field [27]. Since web services might come and go too quickly to allow expert estimates or even collecting historical data on the attack probabilities, assessing vulnerabilities might provide valuable information and extracting probabilities from CVSS data is seen as a promising method: CVSS metrics reflect a strong link between threats, vulnerabilities, and the violation of protection goals. Also, a correlation between the effort in exploiting vulnerabilities and the probability of successful attacks can be assumed. Although CVSS metrics give, strictly spoken, no information about the actual probability of an attack, taking this link into consideration for a risk assessment can be expected to lead to more accurate results than existing methods for estimating attack probabilities. This issue is not yet fully analyzed and subject to further evaluation and research. However, once a suitable method for measuring attack probabilities for IT services should become evident, this could be incorporated into the proposed approach without any methodical change.

3.3. Measures for Protection Goals

In its simplest form, CVSS calculates a score between 0 and 10 for any vulnerability in the database, representing the lowest threat level, 10 the highest. Following the CVSS calculation, the base score is calculated according to the following equation [9]:

$$\text{BaseScore} = \text{round to 1 decimal}(0.6 \cdot \text{Impact} + 0.4 \cdot \text{Exploitability} - 1.5 \cdot f(\text{Impact}))$$ (1)

The components Impact, Exploitability, and $f(\text{Impact})$ are calculated according to the following equations, whereby the absolute numbers are given by the CVSS method:

$$\text{Impact} = 10.41 \cdot (1 - \text{ConfidentialityImpact}) \cdot (1 - \text{IntegrityImpact}) \cdot (1 - \text{AvailabilityImpact})$$ (2)

$$\text{Exploitability} = 20 \cdot \text{AccessVector} \cdot \text{AccessComplexity} \cdot \text{Authentication}$$ (3)

$$f(\text{Impact}) = \begin{cases} 0 & \text{if } \text{Impact} = 0 \\ 1.176 & \text{otherwise} \end{cases}$$ (4)

According to the temporal situation, the BaseScore can be combined with the temporal exploitability values to include information on automated exploits and fixes according to equation (5) and (6):

$$\text{TempBase} = \text{Exploitability} \cdot \text{RemediationLevel} \cdot \text{ReportConfidence}$$ (5)

$$\text{TemporalScore} = \text{round to 1 decimal}(\text{BaseScore} \cdot \text{TempBase})$$ (6)

However, neither the BaseScore nor the TemporalScore show which protection goal(s) the vulnerability under consideration puts at risk. Therefore, an adaptation of the calculation is proposed here for calculating the scores for each protection goal separately. This requires an adaptation of the CVSS values of the impact metrics by replacing equation (2). In order to keep the range of values between 0 and 10, the weights are adapted as follows without changing the basic method of CVSS:

Table 2: Adjusted CIA impact values

<table>
<thead>
<tr>
<th>Metric</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality Impact</td>
<td>none (0), partial (1.7), complete (10)</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>none (0), partial (1.7), complete (10)</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>none (0), partial (1.7), complete (10)</td>
</tr>
</tbody>
</table>
Accordingly, equation (4) is split up and adapted for each of the three protection goals:

\[
\begin{align*}
  f(C\text{Impact}) &= \begin{cases} 
    0 & \text{if } \text{ConfidentialityImpact} = 0 \\
    1.176 & \text{otherwise}
  \end{cases} \\
  f(I\text{mpact}) &= \begin{cases} 
    0 & \text{if } \text{IntegrityImpact} = 0 \\
    1.176 & \text{otherwise}
  \end{cases} \\
  f(A\text{Impact}) &= \begin{cases} 
    0 & \text{if } \text{AvailabilityImpact} = 0 \\
    1.176 & \text{otherwise}
  \end{cases}
\end{align*}
\]

Based on these adjustments, the probability that an exploit of the vulnerability under consideration will harm one of the protection goals can be calculated as follows:

\[
\begin{align*}
  C &= (0.6 \cdot C\text{Impact} + 0.4 \cdot \text{Exploitability} - 1.5) \cdot f(C\text{Impact}) \cdot \text{Temp} \cdot 0.1 \quad \text{with} \quad 0 \leq C \leq 1 \\
  I &= (0.6 \cdot I\text{mpact} + 0.4 \cdot \text{Exploitability} - 1.5) \cdot f(I\text{mpact}) \cdot \text{Temp} \cdot 0.1 \quad \text{with} \quad 0 \leq I \leq 1 \\
  A &= (0.6 \cdot A\text{Impact} + 0.4 \cdot \text{Exploitability} - 1.5) \cdot f(A\text{Impact}) \cdot \text{Temp} \cdot 0.1 \quad \text{with} \quad 0 \leq A \leq 1
\end{align*}
\]

As single services can have several vulnerabilities, multiple CVSS scores must sometimes be combined. Following the approach of [24], the arithmetic average is used as total score. In the case where further information on dependencies between several vulnerabilities is available, e.g. that they can only be exploited in a specific order, this calculation of course can be replaced by more detailed approaches as, e.g., discussed in [26].

### 3.4. Calculation Example

With the adapted CVSS score at hand, every IT service can be assessed regarding its probability of achieving each of the protection goals. This is demonstrated for an exemplary service with three vulnerabilities (see Table 3) which will later be referred to when demonstrating the outstanding economic decision.

<table>
<thead>
<tr>
<th>CVSS metrics</th>
<th>IT Service 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Values</td>
</tr>
<tr>
<td></td>
<td>Vulnerability 1.1</td>
</tr>
<tr>
<td>Access Vector</td>
<td>local (0.395)</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>high (0.35)</td>
</tr>
<tr>
<td>Authentication</td>
<td>none (0.704)</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>partial (1.7),</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>none (0)</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>none (0)</td>
</tr>
<tr>
<td>Exploitability</td>
<td>unproven (0.85)</td>
</tr>
<tr>
<td>Remediation Level</td>
<td>official fix (0.87)</td>
</tr>
<tr>
<td>Report Confidence</td>
<td>unconfirmed (0.9)</td>
</tr>
</tbody>
</table>

The CIA-probabilities of exploitability for IT Service 1 as well as the temporal scores can then be calculated according to equations (3) and (5). Inserting the results into equation (6a), (6b), or (6c), and calculating the corresponding impact with equation (4a), (4b), or (4c), the complete equation...
for the three protection goals can be resolved. Using the exemplary values from vulnerabilities 1.1, 1.2, and 1.3 (see Table 3) leads to the following results.

\[
C = (0.6 \cdot 1.7 + 0.4 \cdot (20 \cdot 0.395 \cdot 0.35 \cdot 0.704) - 1.5) \cdot 1.176 \cdot (0.85 \cdot 0.87 \cdot 0.9) \cdot 0.1 = 0.023
\]

\[
I = (0.6 \cdot 1.7 + 0.4 \cdot (20 \cdot 0.395 \cdot 0.35 \cdot 0.56) - 1.5) \cdot 1.176 \cdot (0.85 \cdot 1.05) \cdot 0.1 = 0.013
\]

\[
A = (0.6 \cdot 1.7 + 0.4 \cdot (20 \cdot 0.395 \cdot 0.35 \cdot 0.45) - 1.5) \cdot 1.176 \cdot (1 \cdot 1 \cdot 0.95) \cdot 0.1 = 0.002
\]

In the same way, the CIA-probabilities for the other IT services can be calculated according to their vulnerabilities. Omitting the detailed values for brevity, the following vulnerabilities and probabilities are assumed.

Table 4: Exemplary services and their vulnerabilities

<table>
<thead>
<tr>
<th>Vuln. #</th>
<th>IT Service 1</th>
<th>IT Service 2</th>
<th>IT Service 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.1</td>
<td>1.2</td>
<td>1.3</td>
</tr>
<tr>
<td>C</td>
<td>0.023</td>
<td>0.029</td>
<td>0.002</td>
</tr>
<tr>
<td>I</td>
<td>0.013</td>
<td>0.011</td>
<td>0.002</td>
</tr>
<tr>
<td>A</td>
<td>0.002</td>
<td>0.014</td>
<td>0.002</td>
</tr>
</tbody>
</table>

Given that vulnerabilities 1.1 to 1.3 can be found in IT Service 1, IT Service 2 has vulnerabilities 2.1 to 2.3, and vulnerabilities 3.1 to 3.6 are related to IT Service 3, the resulting probabilities are shown in Figure 3. To combine the values of several vulnerabilities within one service, the arithmetic average is used as mentioned above. In addition, since low CVSS values stand for a low threat level, the values have to be inverted for getting the aspired probabilities: for example, vulnerability 2.1 in service 2 has a low threat level of 0.029 with regard to confidentiality, i.e. a high probability of 0.971 of achieving that protection goal.

Figure 3: Exemplary services with CIA probabilities

4. Automated Selection of IT Services

The characterization of the IT services according to their capability to achieve the protection goals is only part of the information that is needed for an automated selection between alternative IT services at runtime. The missing part for an economic and value-oriented selection is an assessment of the expected loss for each protection goal in the case of its violation. These values mainly depend on the actual business process that is executed and typically varies from instance to instance. Therefore, the expected losses have to be determined context-specific for each instance. For example, one activity of a purchasing process might require sending a document to the supplier. A box of screws could be ordered with lower confidentiality than a special component that might inform competitors about a new product and thus imply a competitive disadvantage. Bringing together the CIA measures of the IT service with the CIA requirements of the business process facilitates a risk-based selection of the most suitable IT service at runtime. Thus, an orchestration of the IT services ex ante, i.e., when designing the business process, becomes obsolete and, assuming an appropriate extension of the business process model, can be delegated to the business process execution engine.
However, the required assessment of the expected loss in the case of a protection goal violation is a complex task and can hardly be realized by assessing each single activity of a business process that is supported by an IT service. Therefore, a hierarchical model is proposed where elements inherit their values from superordinated elements, e.g., a core process from its superordinated business process. Such hierarchical models are very well known in business process management, e.g., within the framework of British Telecom [11] or the breakdown of business processes through to core processes and detailed processes [15]. If such a uniform “inheritance” is too broad, the values can be adapted on every level and for every instance of the modeled business process as needed.

Equipping each IT service with CIA measures as described in section 3 and each IT supported activity of a business process with corresponding monetary values allows an automated decision between alternative IT services, taking not only costs but also risk into consideration. Then, the expected costs $E$ of an IT service $k$ can be calculated as sum of the direct costs (e.g., for using the service) and indirect costs (e.g., cost of changing between services) $Cost_k$ and the expected loss in the event of a confidentiality breach $LoC$, loss of integrity $LoI$, and non-availability $LoA$:

$$E_k = Cost_k + (1 - C_k) \cdot LoC + (1 - I_k) \cdot LoI + (1 - A_k) \cdot LoA$$  \hspace{1cm} (7)

The expected costs have to be calculated for every IT service that comes into question to support the considered activity of the business process. According to a value-oriented and a risk-neutral decision strategy, the service which results in the lowest expected costs is to be chosen. For demonstration purposes, the example above is revived: a business process activity requires sending a document and there are three functionally identical IT services (e.g., e-mail, Internet form via https, and EDI) available with their CIA measures as described in section 3.4. The direct costs for sending the document amount to 0.01 € for IT Service 1, 0.02 € for IT Service 2, and 1.10 € for IT Service 3. Indirect costs are ignored for keeping the example simple. In the first scenario, when ordering a box of screws, a violation of confidentiality would result in no loss, a violation of integrity would cost 25.00 € due to sending back the wrong box, and non-availability of the service would cost 1.70 €. Calculating the expected costs for each service shows that IT Service 2 is the one to be chosen:

$$E_1 = 0.01€ + (1 - 0.977) \cdot 0.00€ + (1 - 0.987) \cdot 25.00€ + (1 - 0.998) \cdot 1.70€ = 0.34€$$  \hspace{1cm} (8)

$$E_2 = 0.02€ + (1 - 0.971) \cdot 0.00€ + (1 - 0.989) \cdot 25.00€ + (1 - 0.986) \cdot 1.70€ = 0.32€$$

$$E_3 = 1.10€ + (1 - 0.9935) \cdot 0.00€ + (1 - 0.992) \cdot 25.00€ + (1 - 0.9765) \cdot 1.70€ = 1.34€$$

In this scenario, when ordering a special component, where the pure fact of ordering could inform competitors about a new product, a violation of confidentiality would result in a high loss and cost 30,000.00 €, a violation of integrity would also cost 25.00 €, and again, non-availability 1.70 €. In this scenario, the calculation of the expected costs for each service would change to:

$$E_1 = 0.01€ + (1 - 0.977) \cdot 30,000.00€ + (1 - 0.987) \cdot 25.00€ + (1 - 0.998) \cdot 1.70€ = 690.34€$$

$$E_2 = 0.02€ + (1 - 0.971) \cdot 30,000.00€ + (1 - 0.989) \cdot 25.00€ + (1 - 0.986) \cdot 1.70€ = 870.32€$$

$$E_3 = 1.10€ + (1 - 0.9935) \cdot 30,000.00€ + (1 - 0.992) \cdot 25.00€ + (1 - 0.9765) \cdot 1.70€ = 196.34€$$

Thus, it would be advisable to send the order via IT Service 3. Taking only the costs into consideration or fixing an IT service statically to an activity at the moment of business process design would inherently result in a non-optimal selection.

5. Discussion and Outlook

In future SOA, where several alternative IT services are available for realizing activities of business processes, a method is required to select the most suitable one. Statically fixing a specific service to a specific business process activity at design time, or even selecting the IT service dynamically by
only taking costs into consideration, results in a non-optimal selection from a value-oriented view. Therefore, in this contribution, a method for taking riskiness of IT services into consideration has been developed and presented. Protection goals from IT security research, namely confidentiality, integrity and availability are proposed as “risk interface” between the IT service and the business process. A value-oriented selection of IT services requires two extensions: business process models have to be extended with economic values for not achieving protection goals and IT service descriptions have to be extended with measures for achieving these protection goals.

For extending IT service descriptions, CIA measures have been introduced relying on CVSS data. One significant advantage of this approach is that the determination of CIA measures follows a methodic approach and can be automated. It allows the actual relevance of known vulnerabilities to be considered, e.g. if there is a known automated exploit of a vulnerability, this will be reflected in the respective CVSS values and, thus, immediately change the CIA measures of every corresponding IT service. However, there are also several limitations in our approach. One clear subject of further discussion is our interpretation of the CIA measures as probabilities. While a connection between CIA measures and probabilities of violations seem plausible, it remains subject to further research whether this assumption holds or not and how a company’s specific situation can be taken into consideration, e.g., through adjusted CVSS data. However, should a more precise method for calculating actual probabilities of meeting protection goals become available, it would be easy to extend our approach without having to change the whole risk-based selection of IT services. As mentioned above, additional protection goals such as authentication or accountability can easily be included whenever the required information about corresponding vulnerabilities is available.

A further point of discussion is the application of the CIA measures for IT services provided by external suppliers. For IT services integrated from outside the company’s domain, it usually will not be possible to analyze vulnerabilities according to the service and the underlying IT infrastructure. However, the proposed CIA measures can also serve as external metrics that can be monitored without knowing internal metrics of the service itself and thus be integrated into SLA. For calculating the measures, the external service provider has to transform them into internal metrics and this can be achieved by applying the proposed method. In this case, the approach presented has to be extended to cope with the additional trust issues, e.g., by integrating control goals of compliance management – a challenging topic of further research.

**Literature**


