Relating Software Coupling Attribute and Security Vulnerability Attribute

Varadachari S. Ayanam, Frank Tsui, Sheryl Duggins, Andy Wang
Southern Polytechnic State University
Marietta, Georgia 30060

Abstract: Both internal software properties, such as cohesion and coupling, and external software properties, such as performance or security, have been extensively studied [2,11,13]. In this paper we pose a metric for an external property, security vulnerability, using aspects from coupling, which is an internal property. We introduce two metrics, Average Vulnerability (AV) and Degree of Vulnerability (DV), to gauge the extent of security vulnerability. Then these metrics are applied to the top ten security vulnerable components in Mozilla as described by Neuhaus et al [7]. High associations are found between these metrics and the top ten vulnerable components. This result provides a direction that future design review and testing should focus on coupling properties when security is specified as an important factor in the requirements specification.

Keywords: software, coupling, security, vulnerability, metrics

1. Introduction:

Today, information security is one of the dominating news in the IT field where software plays a critical role. Disturbing titles such as “Microsoft Security Advisory: Vulnerability in Microsoft Video Active X Control Could Allow Remote Code Execution” [9] and “Twitter Crippled by Denial-of-Service Attack” [8] are posted on the internet with alarming frequency. Obviously, software assurance requires a well developed process and procedure to produce good quality product; however, in spite of the many efforts in mitigating these security related problems [5, 10], there is clearly room for more work to ameliorate the situation through a better understanding of the inherent relationship between internal software attributes and security.

Software internal attributes such as coupling, cohesion, modularity and complexity are of interest mostly to the software developers and engineers but not so much to the external customers, who are more interested in external attributes such as usability, performance or security. These internal and external software quality attributes are well studied by software engineers [2, 11, 13]. But for the most part, these internal and external attributes have been analyzed independently of each other. We have been investigating these internal software attributes to see if they are related to external software product attributes such as security and how those internal attributes affect the trustworthiness of the product [1, 12, 14].

In this paper we will present the results from our latest research. We introduce a new security-vulnerability metric which demonstrates a general association between the external software attribute of security-vulnerability and the internal attribute of software coupling. This result also supports, in a more general manner, the findings in Liu and Traore [6], who focused on denial-of-service attacks of a medical record keeping system. The two main achievements of our research are: (1) a new security-vulnerability metric that provides empirically similar, but more general, results as others [6, 7] and (2) the new security-vulnerability metric formulation based on the internal attribute of coupling provides a framework of direction for software engineers, when conducting design reviews or developing test cases, to focus more on the software coupling attributes when security-vulnerability attribute is specified as a high priority requirement.

The rest of this paper is presented in three major segments. We first review the fundamental concepts and definitions of coupling and security vulnerability as a source for constructing metrics for projecting vulnerability. Second, new security-vulnerability metrics, Average
Vulnerability (AV) and Degree of Vulnerability (DV), are then developed within the context of the well understood internal software coupling attributes. Finally, utilizing the new metric and empirical data from Neuhaus et al [7], we show that security-vulnerability measured through coupling-based metrics, AV and DV, demonstrate similar association as what was found in [7], thereby giving some empirical credence to the new metrics.

2. Software Security and Coupling Attributes:

Software security is one of the most important external, quality attributes that is of concern to both software developers and end users these days. Hogland and McGraw [3] define software security as the ability to defend attacker’s exploitation of software problems by building software to be secure throughout the development cycle. Software vulnerability is a weakness in a software system that allows an attacker to use the system for a malicious purpose. Ivan Krsul [4] defined software vulnerability as an instance of a “fault” in the specification, development, or configuration of software such that its execution can violate an implicit or explicit security policy. Stated a bit differently, vulnerability refers to flaws or weaknesses in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy. Any flaw or weakness in an information system could be exploited or attacked.

"Attackability," according to Liu and Traore [6], is a measure of the extent that a software system or service could be the target of successful attacks. Thus attackability may be viewed as an indicator of vulnerability. Vulnerability can come from design flaws, implementation errors, configuration errors and other sources. Early detection and mitigation of vulnerabilities in software through design reviews can help produce higher quality and more secure software. One should also prioritize testing efforts of these vulnerabilities and reduce the cost of later fixes. There is evidence that shows internal attributes, such as coupling, may be a source of vulnerability and thus attackability [6].

Coupling is one of the traditional internal software quality attributes that affects overall software quality [11]. Coupling is related to “sharing” or interaction among software entities and components. There are five levels of severity of coupling: (1) content, (2) common, (3) control, (4) stamp, and (5) data coupling. These are listed in the order of severity level from high to low, where the highest severity level, (1), is viewed as tightest coupling and thus the worst based on current software engineering principles. It is rare that a software package can be developed without one or more of these types of coupling. However, it is well accepted that the most severe level or the worst type of coupling, content coupling, is to be avoided as much as possible. Regardless of the type of coupling, when information is passed among components there is high potential that it is also exposed. That is, there is a potential that the information may be intercepted or altered by unintended parties. Coupling may be considered a “flaw” in the design or a source of software vulnerability. Thus, intuitively, coupling should be considered a factor that can affect software security. Ayanam [1] has also shown that many forms of SQL injection or buffer overflow attacks are based on exploitations of certain types of coupling. It makes sense to also assume that the severity level or type of coupling of a software product should have an impact on the severity of its security vulnerability or its attackability.

3. Vulnerability Metrics:

In this section, we devise a metric to use for studying the association between coupling and vulnerability. The traditional severity level or types of coupling from content coupling to data coupling will be included in characterizing the impact of coupling to security vulnerability. We first define an Average Vulnerability metric, AV, based on the traditional five basic types of coupling as follows:

\[
AV = \sum w_i C_i \tag{1}
\]

a) i ranges from 1 through 5 , indicating the five types of coupling,
b) \(C_i\) is the number of instances of i type of coupling and
c) \(w_i\) is the weight assigned to the i type of coupling

The weights we used reflect and preserve the traditional order of coupling. That is content coupling is given the highest weight because it is viewed as the worst kind of coupling and the weight decreases respectively to the lowest for weight for data coupling. After experimenting with different weights, we settled on giving \(w_1\)
the value of 3, \( w_2 \) is assigned 2.5, \( w_3 \) is assigned 2.0, \( w_4 \) is assigned 1.5 and \( w_5 \) is assigned 1.0. Note that we made an assumption that the type of coupling decreases in an equal amount of .5. Clearly, different intervals will affect the measurement. However, much more research on coupling is needed before a definitive set of intervals can be assumed as the standard. For now we chose to use the simplified assumption of equal intervals. AV can range in value from 0 to some very large number. The question is how large is very large vulnerability? We need some sense of the scale of vulnerability, and AV does not provide that. Thus a little more elegant metric called Degree of Vulnerability, DV, is defined as follows.

\[
DV = 1 - \left( \frac{1}{AV} \right) \quad \text{where } 0 \leq DV < 1 \quad (2)
\]

Note that DV provides a scale and ranges from 0 to a value less than 1. When the DV value approaches 1, it indicates that the software system is highly vulnerable to security attacks because AV is large. When AV has only one occurrence of data coupling, \( AV = 1 \). This is viewed as the minimal coupling for any realistic software system, and DV will be zero. In the rare event that a software system actually has no occurrence of coupling where \( AV = 0 \), we still define AV as 1.

In the next section we will utilize these metrics and analyze data from real projects obtained from Neuhaus, et al [13].

4. Analysis with Real Empirical Project Data:

We have chosen Mozilla database for our empirical study because Mozilla bugs and sources are freely available and also because Neuhaus, et al [7] have used Mozilla to come up with the Top 10 most vulnerable components in their study. In this section we will use the raw data obtained from Neuhaus et al [7], together with our calculated AV and DV metrics to a) show empirical evidence between Coupling and Vulnerability and b) show that AV and DV, via coupling attributes, can be used as metrics for assessing security-vulnerability.

<table>
<thead>
<tr>
<th>Top 10 Most Vulnerable</th>
<th># of Bug Report</th>
<th>AV metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>jsobj.c</td>
<td>24</td>
<td>339.5</td>
</tr>
<tr>
<td>nsCSSFrameConstructor.cpp</td>
<td>17</td>
<td>60</td>
</tr>
<tr>
<td>jsfun.c</td>
<td>15</td>
<td>150.5</td>
</tr>
<tr>
<td>nsScriptSecurityManager.cpp</td>
<td>15</td>
<td>35.5</td>
</tr>
<tr>
<td>NsGlobalWindow.cpp</td>
<td>14</td>
<td>116.5</td>
</tr>
<tr>
<td>jcsript.c</td>
<td>14</td>
<td>165.5</td>
</tr>
<tr>
<td>jsinterp.c</td>
<td>14</td>
<td>163.5</td>
</tr>
<tr>
<td>nsDOMClassinfo.cpp</td>
<td>10</td>
<td>124.5</td>
</tr>
<tr>
<td>nsGenericElement.cpp</td>
<td>10</td>
<td>131.5</td>
</tr>
<tr>
<td>nsDOCSHELL.cpp</td>
<td>9</td>
<td>57.5</td>
</tr>
</tbody>
</table>

Table 1 lists the top 10 vulnerable components of Mozilla database [7], ordered by bug reports. We also listed the associated AV metric for these top ten components. We computed the Pearson Correlation Coefficient between the top ten components and the AV metrics. We also computed the Spearman Ranked Correlation coefficient. The Pearson Correlation Coefficient was 0.66. This implies a relatively strong relation between security-vulnerability and general coupling as AV metric is expressed in terms of the five types of coupling. The Spearman Ranked Correlation came out to be 0.235. The Spearman Rank Correlation of 0.235 implies that the ranking of the components by number of bugs and the ranking of components by the number of two types of coupling studied explicitly by Neuhaus et al (import- stamp coupling and function calls – control coupling in [7] ) do not show high association. The following possible reasons can be attributed to the low Spearman Rank Correlation:

- The coupling rank interval, assumed to be of equal interval of .5, may be erroneous and needs further study and adjustments
- We considered only the top 10 most vulnerable components of Mozilla. Had we included more components the result could have been different.

From the Pearson and Spearman Rank correlations we can infer that the high-level, general picture of coupling and amount of bugs may be associated, but the detailed ranking may not. Next, DV metric is computed for the same
Recall that DV can range in value from 0 to 1. All DV metric values in Table 2 are extremely high. They are greater than 0.9 for all of the top ten vulnerable components. The DV values here all approach the limit value of 1. Thus the DV values properly represented the potential security vulnerability and the high potential of attackability of these components. Since DV metric represents the degree of security vulnerability expressed in terms of coupling, high DV metric implies high software coupling in these security vulnerable components of Mozilla. This result also substantiate the results found in [6,7].

5. Conclusion:
In this paper we introduced two new software security vulnerability metrics, AV and DV, based on internal software coupling attribute. These metrics were shown to have high association with the top ten security vulnerable components in Mozilla as described by Neuhaus et al [7]. This relationship with real empirical data makes both AV and DV metrics a good candidate as a future tool for assessing security vulnerability. Also, this successful usage of internal software attribute, coupling, to assess an external software attribute, security, provides a direction for future software design reviews and testing to focus on coupling as a necessary attribute of interest when the requirements document indicates a need for high level of security. More study is still needed in the future in fine tuning the AV metric. Specifically, our simplified approach of using equal intervals of .5 to differentiate the levels of coupling resulted in low Spearman Ranked Correlation. This indicates that these coupling intervals are clearly not uniform. We plan to use more empirical data to further analyze the different coupling intervals in relationship to different levels of security vulnerability.

6. References: