An Empirical Methodology to Evaluate Vulnerability Discovery Models

Fabio Massacci and Viet Hung Nguyen

Abstract—Vulnerability Discovery Models (VDMs) operate on known vulnerability data to estimate the total number of vulnerabilities that will be reported after a software is released. VDMs have been proposed by industry and academia, but there has been no systematic independent evaluation by researchers who are not model proponents. Moreover, the traditional evaluation methodology has some issues that biased previous studies in the field. In this work we propose an empirical methodology that systematically evaluates the performance of VDMs along two dimensions (quality and predictability) and addresses all identified issues of the traditional methodology. We conduct an experiment to evaluate most existing VDMs on popular web browsers’ vulnerability data. Our comparison shows that the results obtained by the proposed methodology are more informative than those by the traditional methodology. Among evaluated VDMs, the simplest linear model is the most appropriate choice in terms of both quality and predictability for the first 6 – 12 months since a release date. Otherwise, logistics-based models are better choices.

Index Terms—Software Security, Empirical Evaluation, Vulnerability Discovery Model, Vulnerability Analysis

1 INTRODUCTION

Time-based vulnerability discovery models (VDMs) are parametric functions counting the total number of vulnerabilities of a software at an arbitrary time \( t \). For example, if \( \Omega(t) \) is the cumulative number of vulnerabilities at time \( t \), the function of the linear model (LN) is \( \Omega(t) = At + B \) where \( A, B \) are parameters of LN, which are estimated from historical vulnerability data.

VDMs can be seen as a specialization of Software Reliability Growth Models (SRGMs) which were proposed to forecast the total number of defects in a software that could be found as a consequence of testing and debugging procedures [17], [51], [26]. The purpose of a VDM is not to identify vulnerable components (as defect prediction papers do e.g., [29], [42], [15]) but to evaluate the security profile of the software as a whole. Accurate VDMs can be used by software vendors and users to understand security trends, plan patches and updates, forecast security investments, or decide which open source software to bundle with one’s own products.

VDMs were initially based on the same principles behind SRGMs. Yet, empirical evidence (in the reported literature and this paper) shows that functions which describe laws for vulnerabilities differ from laws for software bugs SRGMs. For example, Anderson’s Thermodynamic (AT) model [8] was one of the first VDM and is explicitly based on SRGM concepts. Yet, it is the worst model in terms of fitting empirical data. Some authors argued that such difference is due to sociological factors [2], [28]: the drop in rate of discovery can be explained by a drop in interest about a software version rather than by the increased difficulty of finding vulnerabilities. Independent experiments showed that many vulnerabilities reported for new versions of a software were indeed present in its previous versions [36], [22].

Fig. 1 sketches a taxonomy of major VDMs, which could be classified into two categories: time-based and effort-based. The former measures the total number of vulnerabilities in the course of time, as previously discussed. The latter counts vulnerabilities regard to the testing effort. This work focuses on time-based VDMs, which were also the major concern of most VDM papers in the literature. Apart from the simplest linear model (LN) [4], and Logarithmic Poisson (LP) model, time-based VDMs (at the time of writing this paper) include Anderson’s Thermodynamic (AT) model [8], Rescorla’s Quadratic (RQ) and Rescorla’s Exponential (RE) models [39], Alhazmi & Malaia’s Logistic (AML) model [2], AML for Multi-version (MVDM) model [19], Weibull model (JW) [18], and Folded model (YF) [53]. Hereafter, we shortly refer to time-based VDM as VDM.

There are two fundamental questions in past VDM papers: “how well does a VDM fit the data?”, and “which model is better than another?”. 
Many studies tried to address these questions but the used methodologies suffer from a number of issues that we document at length in Section 3. In summary:

1) Most past studies do not clearly specify what counts as one vulnerability. While the conceptual notion of vulnerability as a software bug is well understood [20], [35], VDM papers counted entries in vulnerability databases. Example 1 and Fig. 2(a) in Section 3.2 show how the same conceptual vulnerability could count as 1 or 3 depending on which database is chosen. Different counts may favor different VDMs.

2) Some studies (e.g., [47], [49]) considered all versions of a software as a single entity. They belong to a product line, but differ by non-negligible amount of code. Considering them as a single entity makes the evaluation imprecise (e.g., Fig. 2(b)).

3) The methodology used in the literature estimates the parameters of a VDM by using all available vulnerability data (at the time of the writing of the paper). This is in sharp contrast with defect prediction techniques in software engineering (e.g., [29], [42], [16]) where only a part of the data is used for fitting, another part is used for validation (e.g., cross-validation, next-release validation). For example, while fitting AML to the data set of Win2K vulnerabilities, the experiment in [6] reported a significance level \( p\text{-value} = 0.44 \), which could be positive; whereas \( p\text{-value} = 0.05 \) in [7], which is definitely bad. Barring errors, this can only be explained by the (misleading) methodology.

4) The \( p\text{-value} \) of a statistical test tells us the chance that the estimated model is different from the data. If \( p\text{-value} \geq 0.05 \), past papers concluded the model well fits the data. Lower \( p\text{-value}\)-values can be soundly used to reject a bad model, but being barely over the threshold is overly optimistic to conclude a model is good. Further, a model is not just “valid” or “invalid”. Models have evidence in their favor, and evidence against them. Reporting a single value may obscure temporal properties (e.g., best in the first 6 months since release).

5) Moreover, no study used VDMs as a predictor, for example, to forecast data for the next quarter.

We proposed an empirical methodology to assess the empirical performance of VDMs. The methodology consists of two quantitative metrics, quality and predictability, and a fully guided process. To evaluate the methodology we apply it to some appropriate domain. In the past, researchers chose operating systems as target applications to evaluate VDMs, but paid little attention to other software classes. Nowadays, web browsers are one of the most important internet applications, and are the products with most vulnerabilities, besides operating systems [52]. According to Google [38] more than two-third of attacks to internet users exploit vulnerabilities of browsers or their plug-ins.

We demonstrated the methodology by analyzing the AML, AT, JW, RQ, RE, LP, LN and YF models on Internet Explorer (IE), Firefox, Chrome, and Safari. We selected all major releases which had at least one year of vulnerability data till the collection date.

The experiment reveals interesting findings (TABLE 1): the AT and RQ models are not adequate; the traditional methodology used the maximum horizon of 36 months and allowed a mediocre model (JW/YF) to apparently outperform better but specialized models (LN,AML) that only applied for a limited time span. Such comparison was not done in past studies, because the traditional evaluation methodology did not allow it as VDMs were fitted to a single horizon.

In the next section (§2) we present the terminology. Then we review related work and discusses how they impact our study (§3). Section 4 details our proposed methodology. Section 5 reports the vulnerability acquisition for browser vulnerabilities and Section 6 the evaluation experiment of VDMs on browsers. Section 7 compares the proposed methodology to the traditional one using the experiment results. Last we discuss the threats to the validity (§8) and conclude this work (§9).

2 TERMINOLOGY

- A vulnerability is “an instance of a [human] mistake in the specification, development, or configuration of software such that its execution can [implicitly or explicitly] violate the security policy”[20], later revised by [35]. The definition covers all aspects of vulnerabilities discussed in [9], [10], [13], [40].
- A data set is a collection of vulnerability data extracted from one or more data sources.
- A release refers to a version of an application e.g., Firefox v1.0. A release is considered as a major release depending on its vendor’s version numbering scheme. For example the version numbers of Firefox major releases include 1 decimal digit (e.g., Firefox v1.5, v3.5), whereas the others browsers use only digits before the decimal (e.g., Chrome v1, IE v4). We follow software vendors’ decision on what a major release is (see Section 4.1).
- A horizon is a specific time interval sample. It is version by the number of months since the release date, e.g., 12 months since the release date.
3 Related Work

We recap studies about SRGMs, VDMs, and defect prediction models to highlight similarities and differences. Then we perform a complete review of VDMs studies.

3.1 SRGMs and Defect Prediction Models

SRGM papers try to predict the defect (or bug) discovery rate in a software product by its own developers, as a proxy for the software failure rate [17]. The first and most representative example by Goel and Okumoto [17] has two parameters: the expected total number of defects, and the rate at which the defect discovery rate decreases. The researchers assume that finding bugs become exponentially harder as time goes by. Yamada et al. [49] used the gamma function instead of the exponential one. Musa et al. [51] proposed the LP model, which assumed an infinite number of bugs. For a discussion about SRGMs, interested readers are referred to [50].

VDMs can be seen as a specialization of SRGMs which focus on security bugs. Yet, this paper and a number of studies [6], [2], [7], [5] showed that VDMs based on SRGMs are empirically inadequate.

The need to consider security defect distinctly from ordinary software bugs has been argued by a number of authors. Roger Needham [28] claimed that security bugs are different from ordinary bugs, “not for a technical but a social reason” because “if a security bug is found in a system there is a community of people who make their personal priority to make the wrong behavior happen, typically in other people’s computers”. This adversarial process makes the vulnerability discovery process different from normal bug finding as Alhazmi and Malaiya also advocated [2]. At first, people need time to study the software, so they discover few vulnerabilities. When they understand the software, they rapidly discover many vulnerabilities. Finally, the discovery process flattens not because vulnerabilities are harder to find but rather because people lose interest in finding them.

To capture the above phenomenon Alhazmi and Malaiya proposed a logistic, s-shaped model in their seminal paper [2]. The AML model has been evaluated in several applications spanning in various software classes (TABLE 3), such as operating systems [6], [2], [7], [5], server applications [3], [48], [49], and browsers [47]. Our study [22] showed that vulnerabilities found for the current version may, as a by-product, affect earlier versions thus generating an increase of “after-life” vulnerabilities, i.e. vulnerabilities of a version that has long gone out of support. The presence of after-life vulnerabilities may explain why we do not find a strong empirical evidence that the curve may flatten at the end.

The LN model was firstly proposed as a VDM by Alhazmi and Malaiya [4]. In [4], they analyzed AML and LN models in Windows 98/2K and RedHat Linux 7.1. Rescorla [39] proposed RQ and RE models. He evaluated them on WinNT 4.0, Solaris 2.5.1, FreeBSD 4.0 and RedHat 7.0. Rescorla discussed many shortcomings of National Vulnerability Database (NVD), but his study still heavily relied on it. We partially address these shortcomings by taking into account other data sources.

Joh et al. [18] proposed JW model, and compared it to AML on WinXP, Win2K3 and Linux (RedHat and Red-Hat Enterprise). The goodness-of-fit of JW was slightly worse than AML. In other work, Younis et al. [53] proposed YF model and compared it to AML on Win7, OSX 5.0, Apache 2.0, and IE8. The paper claimed that YF was somewhat better than AML.

Kim et al. [19] introduced AML for Multiple-Version (MVDM), a generalization of AML. It divides vulnerabilities of a version into several fragments. The first fragment includes vulnerabilities affecting this version and past versions, and other fragments include shared vulnerabilities. The authors compared MVDM to AML on Apache and MySQL.

Defect prediction papers aim at predicting whether a source entity (e.g., method, file, component) has a defect. In contrast to SRMGs, they typically try to predict individual vulnerable components based on some characteristics of the software components. For instance, some papers used code churn [27], [15], library import patterns [29], code metrics [34], [42], [11], dependencies [54], [32]. These models were often evaluated by two techniques: cross-validation, and next-release (or future) prediction. The former divides the data into k folds, then uses k – 1 folds as the training set, and 1 fold as the testing set. The latter, as its name suggested, divides the data by the versions affected by defects, then uses data of older versions as the training set, and data of newer ones as the testing set. Such approach is not used in past VDMs studies.

3.2 An Analysis of the VDMs Evaluation Results

TABLE 2 summarizes the methodology used in VDM evaluation studies whereas TABLE 3 summarizes the evaluation results. In TABLE 2 each study is reported with its target VDMs and the classes of software applications used to conduct the experiment. The table also reports the evaluation methodology of the studies. VDMs have been evaluated in several software classes spanning from server applications, browsers, to operating systems. We briefly discuss some of the issues behind the methodological choices behind these studies.

**Vulnerability Count Methods**

Most of past studies (see TABLE 2) did not clarify exactly what was counted as one vulnerability, and what considered as one vulnerable software. Since the purpose
of a VDM is to estimate the **number** of bugs, this lack of clarity can make reported results difficult to reproduce.

For example, one vulnerability count could be either an advisory report by software vendors (e.g., Mozilla Foundation Security Advisories – MFSA), or a security bug causing software to be exploited (e.g., Mozilla Bugzilla), or an entry in third-party data sources (e.g., an NVD entry, or CVE, alternatively). A VDM could perfectly fit data counts using a data source, but poorly fit data counts using different data sources.

**Example 1** In Fig. 2(a), a flaw concerning a buffer overflow in Firefox v13.0 is reported as 1 MFSA entry (MFSA-2012-40), 3 Bugzilla entries (744541, 747688, and 750066), and 3 CVEs entries (CVE-2012-1947, CVE-2012-1940, and CVE-2012-1941). The directional connections illustrate cross references among entries.

**Example 2** Fig. 2(b) visualizes the second fold of this issue in a plot of the cumulative vulnerabilities of Firefox v1.0, Firefox v1.5, and Firefox v1.0-1.5 as a single entity. Clearly, the function of the “global” version is different from the functions of the individual versions.

**Example 3** AML and JW curves fitted the ‘bundled’ Linux data set (i.e., all versions as a single entity) but the models fitted for the single versions v6.0 and v6.2 were statistically different [18].

One could consider all 114 versions of Chrome 35.0.1916.1, ..., 35.0.1916.114 as separate entities instead of the major version Chrome 35.0. The notion of VDM would be meaningless as every version would have a minuscule lifetime. Further, all minor versions are typically

---

TABLE 2
Summary of VDM evaluation studies.

<table>
<thead>
<tr>
<th>Study</th>
<th>Validated VDM</th>
<th>Software Class</th>
<th>Fit Model</th>
<th>GoF test</th>
<th>Predictability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFSA 750066</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFSA 744541</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFSA 747688</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFSA 750066</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFSA 744541</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFSA 747688</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFSA 750066</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

TABLE 3
Validation Method

<table>
<thead>
<tr>
<th>Validation Method</th>
<th>Study</th>
<th>Software Class</th>
<th>Fit Model</th>
<th>GoF test</th>
<th>Predictability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

The arrow-headed lines indicates the cross-references between entries. One conceptual flaw is counted differently in three databases. These counts are all legitimate. So what should we choose?
released mainly to fix (security) bugs in a major release, and are unlikely to introduce new vulnerabilities. Thus, we consider only major releases.

Choice of the Statistical Test

Most of studies (see TABLE 2) shared a common evaluation methodology which fitted VDMs to a single time horizon of collected vulnerability data. They used $\chi^2$ test to determine whether a VDM fits actual data. If the test returned $p$-value $\geq 0.05$, they claimed the VDM to be a good fit to the data. TABLE 3 summarizes the evaluation results for VDMs. This table reports the $p$-values returned by the goodness-of-fit test between generated curves and actual data as reported in the cited papers. In TABLE 3, $p$-values greater than or equal 0.80 (i.e., good fit) are bold, $p$-values between 0.05 and 0.80 (i.e., what we consider an inconclusive fit, but some authors considered a good fit) are reported in italic. The remaining values with $p$-values lower than 0.05 are normally considered a poor fit by statistical tests. The $\chi^2$ test seems to be the most appropriate one among other goodness-of-fit tests, such as the Kolmogorov-Smirnov (K-S) test, and the Anderson-Darling (A-D) test. The K-S test is an exact test, but only applies to continuous distributions and the parameters of the distribution cannot be estimated from the data. Hence, we cannot apply it to perform the goodness-of-fit test for a VDM. The A-D test is a modification of the K-S test that works for some distributions [33, Chap. 1], but some VDMs violate its assumption.

Some studies [2], [5] employed Akaike Information Criteria (AIC) [1], which measures the relative quality of a statistical model for a given data set, to compare VDMs. However, AIC gives no information about the absolute quality. It thus cannot be used to determine the goodness-of-fit of VDM. Moreover, AIC varies with the number of free parameters of a VDM. A model with more free parameters naturally has an advantage in AIC.

Therefore, we do not use AIC, but rely on the $\chi^2$ test in our methodology because it yields comparable results between traditional analysis and ours (when the horizon is the largest data set available).

The second issue is the choice of the value to claim that a VDM was a good fit to a data set. Most studies reported that a model was a good fit when the $\chi^2$ test returned $p$-value $\geq 0.05$. Statisticians use a $p$-value lower 0.05 to reject a model but it does not mean that models with a higher value are good.

We avoid this pitfall by using the statistical practice of selecting good models with an acceptance threshold of 0.80 [24, Chap.8]. A $p$-value between the acceptance threshold of 0.8 and the rejection value of 0.05 means that evidence is inconclusive. Since a model may obtain a good fit on some data, a bad fit on other data, and an inconclusive fit elsewhere we propose an inconclusiveness contribution factor $\omega$ as a mean to study the impact of inconclusive VDM in the quality analysis (§4.2).

Model Fitness as a Single Data Point

Previous studies took a snapshot of vulnerability data, and fitted VDMs to this entire snapshot. The single $p$-value result of this fitting process was used to directly conclude whether a model was “better” than another. At first, this brittle claim only evaluates a model at a single time point (of writing of the paper) and not how this valuation may change over time. This makes repeatability and comparison of experiments difficult. Second, it might allow mediocre models (just barely adequate throughout a product lifetime) to get a better score that specialized models (very good but only for a part of a product’s lifetime).

Example 4 In TABLE 3 AML definitely fitted Win98 in [48], [49] ($p$-value = 1, essentially a perfect prediction), but inconclusively fitted it in [6] ($p$-value = 0.74) and [7] ($p$-value = 0.21). The $p$-values that AML fitted Win2K vulnerabilities in [6], [7] were 0.44 and 0.05, respectively. While the former is inconclusive, the latter is essentially reject (i.e., the model is totally unrelated to the data).

This is a clear evidence that the goodness-of-fit of a model is changing over time. So, we report the values of VDM goodness-of-fit as a function of time.

Maximal Horizon vs Training and Test Time Horizons

The traditional procedure for VDMs evaluation (all data is training data) has an additional drawback. It is in sharp contrast with the standard procedure used by defect prediction approaches (separating data into training and testing sets) and does not tell us anything about the ability of VDMs to be a good “law of nature” that is able to predict extent the future.

The predictability of VDMs was also discussed in some studies [3], [49], [53] by exploiting two measures, namely Average Error (AE) and Average Bias (AB) [21]. However the application of AE and AB in these studies was inappropriate. The authors used a VDM fitted to the data observed at time $t_{max}$, and measured its “predictability” at time $t_i < t_{max}$. In other words, this is hardly ‘prediction’ in the common sense.

We avoid the above pitfall by analyzing the predictability of VDMs in a natural way. Concretely, we fit a VDM to the data observed at time $t_0$, and use the fitted model to evaluate against data observed at time $t_j > t_0$.

4 Methodology

In this work, we address the following two questions:

- **RQ1** How to evaluate the performance of a VDM?
- **RQ2** How to compare between two or more VDMs?

TABLE 4 summarizes the key steps of our methodology to answer the research questions, while addressing the issues discussed in the related work section.
4.1 Step 1: Acquire Vulnerability Data

We classify data sources used to study VDMs for software products. In the sequel software vendor is the company or institute that develop the software product(s).

- Third-party advisory (TADV): is a vulnerability database maintained by a third-party organization (not the software vendor) e.g., NVD, Open Source Vulnerability database (OSVDB), etc.
- Vendor advisory (ADV): is a vulnerability database maintained by the software vendor, e.g., MFSA, Microsoft Security Bulletin. Vulnerability information in this DB has been always evaluated by the vendor.
- Vendor bug tracker (BUG): is a bug-tracking database, usually maintained by the vendor.

For our purposes, a vulnerability data entry must have the following minimal features:

- Identifier (id): is the identifier of a vulnerability.
- Disclosure date (date): refers to the date when a vulnerability is reported to the database.
- Vulnerable Releases (R): is a list of releases affected by a vulnerability.

We also report Firefox’s vulnerabilities, but most of them refer to NVD by the CVE-ID. Therefore, we consider NVD as a representative of third-party data sources.

Example 5 Vulnerabilities of Firefox are collected from three data sources: NVD, MFSA, and Mozilla Bugzilla. Neither MFSA nor Bugzilla provides the Vulnerable Releases feature, but NVD does. Each MFSA entry has links to NVD and Bugzilla. We combine these data sources to obtain the missing data.

TABLE 3
Summary of VDM evaluation results (p-values) in the literature.

<table>
<thead>
<tr>
<th>Study</th>
<th>Model</th>
<th>Year</th>
<th>Year</th>
<th>Browser</th>
<th>DBMS</th>
<th>Operating System</th>
<th>Web Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>[6]</td>
<td>2005</td>
<td>2005</td>
<td>Firefox</td>
<td>0.44</td>
<td>1.00 0.74 0.92 0.96</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[2]</td>
<td>2005</td>
<td>2005</td>
<td>IE 8</td>
<td>1.00</td>
<td>1.00 0.92 0.96</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[3]</td>
<td>2006</td>
<td>2006</td>
<td>Mozilla</td>
<td>0.99</td>
<td>1.00 0.99 0.05 0.05</td>
<td>1.00 0.21 0.92 0.32</td>
</tr>
<tr>
<td></td>
<td>[48]</td>
<td>2006</td>
<td>2006</td>
<td>MySQL</td>
<td>0.83</td>
<td>0.81 0.85 0.83 0.66 0.96</td>
<td>1.00 0.94</td>
</tr>
<tr>
<td></td>
<td>[47]</td>
<td>2006</td>
<td>2006</td>
<td>FreeBSD.4.0</td>
<td>0.00</td>
<td>0.98 0.70</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[7]</td>
<td>2007</td>
<td>2007</td>
<td>CentOS 5</td>
<td>0.98</td>
<td>0.70</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[19]</td>
<td>2007</td>
<td>2007</td>
<td>RH Fedora</td>
<td>0.99</td>
<td>0.73</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[5]</td>
<td>2008</td>
<td>2008</td>
<td>RH Linux 6.0</td>
<td>0.99</td>
<td>0.73</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[18]</td>
<td>2008</td>
<td>2008</td>
<td>RH Linux 7.0</td>
<td>0.99</td>
<td>0.73</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[49]</td>
<td>2011</td>
<td>2011</td>
<td>Apache 2.1</td>
<td>0.99</td>
<td>0.73</td>
<td>1.00 1.00 1.00</td>
</tr>
<tr>
<td></td>
<td>[53]</td>
<td>2011</td>
<td>2011</td>
<td>Win2K</td>
<td>0.99</td>
<td>0.73</td>
<td>1.00 1.00 1.00</td>
</tr>
</tbody>
</table>

*: the validation experiment is conducted by people who are not (co-)authors of the corresponding model.
## TABLE 4
Methodology overview.

<table>
<thead>
<tr>
<th>Step 1 Acquire the vulnerability data</th>
<th><strong>DESC.</strong></th>
<th>Identify the vulnerability data sources, and the way to count vulnerabilities. If possible, different vulnerability sources should be used to select the most robust one (e.g., vendor confirmed ones). Observed samples then can be extracted from collected vulnerability data.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>INPUT</strong></td>
<td>Vulnerability data sources.</td>
</tr>
<tr>
<td></td>
<td><strong>OUTPUT</strong></td>
<td>Set of observed samples.</td>
</tr>
</tbody>
</table>
|                                       | **CRITERIA** | **CR1** Collection of observed samples  
- Vulnerabilities should be counted for individual releases (possibly by different sources).  
- Each observable sample should have at least 6 data points. |

<table>
<thead>
<tr>
<th>Step 2 Fit the VDM to observed samples</th>
<th><strong>DESC.</strong></th>
<th>Estimate the parameters of the VDM formula to fit observed samples as much as possible. The $\chi^2$ goodness-of-fit test is employed to assess the goodness-of-fit of the fitted model based on criteria <strong>CR2</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>INPUT</strong></td>
<td>Set of observed samples.</td>
</tr>
<tr>
<td></td>
<td><strong>OUTPUT</strong></td>
<td>Set of evaluated samples.</td>
</tr>
</tbody>
</table>
|                                       | **CRITERIA** | **CR2** The classification of the evaluated samples based on the p-value of a $\chi^2$ test.  
- **Good Fit**: $p$-value $\in [0.80, 1.0]$, a good evidence to accept the model. We have more than 80% chances of generating the observed sample from the fitted model.  
- **Not Fit**: $p$-value $\in [0, 0.05]$, a strong evidence to reject the model. It means less than 5% chances that the fitted model would generate the observed sample.  
- **Inconclusive Fit**: $p$-value $\in [0.05, 0.80]$, there is not enough evidence to neither reject nor accept the fitted model. |

<table>
<thead>
<tr>
<th>Step 3 Perform goodness-of-fit quality analysis</th>
<th><strong>DESC.</strong></th>
<th>Analyze the goodness-of-fit quality of the fitted model by using the temporal quality metric which is the weighted ratio between fitted evaluated samples (both <strong>Good Fit</strong> and <strong>Inconclusive Fit</strong>) and total evaluated samples.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>INPUT</strong></td>
<td>Set of evaluated samples.</td>
</tr>
<tr>
<td></td>
<td><strong>OUTPUT</strong></td>
<td>Temporal quality metric.</td>
</tr>
</tbody>
</table>
|                                               | **CRITERIA** | **CR3** The rejection of a VDM.  
A VDM is rejected if it has a temporal quality lower than 0.5 even by counting **Inconclusive Fit** samples as positive (with weight 0.5). Different periods of software lifetime could be considered:  
- 12 months (young software)  
- 36 months (middle-age software)  
- 72 months (old software) |

<table>
<thead>
<tr>
<th>Step 4 Perform predictability analysis</th>
<th><strong>DESC.</strong></th>
<th>Analyze the predictability of the fitted model by using the predictability metric. Depending on different usage scenarios, we have different observation periods and time spans that the fitted model supposes to be able to predict.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>INPUT</strong></td>
<td>Set of evaluated samples.</td>
</tr>
<tr>
<td></td>
<td><strong>OUTPUT</strong></td>
<td>Predictability metric.</td>
</tr>
</tbody>
</table>
|                                       | **CRITERIA** | **CR4** The observation period and prediction time spans based on some possible usage scenarios (in browsers).  
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Observation Period (months)</th>
<th>Prediction Time Span (months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short-term planning</td>
<td>6–24</td>
<td>3</td>
</tr>
<tr>
<td>Medium-term planning</td>
<td>6–24</td>
<td>6</td>
</tr>
<tr>
<td>Long-term planning</td>
<td>6–24</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5 Compare VDMs</th>
<th><strong>DESC.</strong></th>
<th>Compare the quality of the VDM with other VDMs by comparing their temporal quality and predictability metrics.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>INPUT</strong></td>
<td>Temporal quality and predictability measurements of models in comparison.</td>
</tr>
<tr>
<td></td>
<td><strong>OUTPUT</strong></td>
<td>Ranks of models.</td>
</tr>
</tbody>
</table>
|                     | **CRITERIA** | **CR5** The comparison between two VDMs  
A VDM $vdm_1$ is better than a VDM $vdm_2$ if:  
- either the predictability of $vdm_1$ is significantly greater than that of $vdm_2$,  
- or there is no significant difference between the predictability of $vdm_1$ and $vdm_2$, but the temporal quality of $vdm_1$ is significantly greater than that of $vdm_2$.  
The temporal quality and predictability should have their horizons and prediction time spans in accordance to criteria **CR3** and **CR4**. Furthermore, a controlling procedure for multiple comparisons should be considered. |
TABLE 5
Formal definition of data sets.

<table>
<thead>
<tr>
<th>Data set</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVD(r)</td>
<td>{nvdr \in NVD \mid r \in R_{med}}</td>
</tr>
<tr>
<td>NVD.Bug(r)</td>
<td>{nvdr \in NVD \mid \exists b \in BUG : r \in R_{nvdr} \land \exists b \in refs_{nvdr}}</td>
</tr>
<tr>
<td>NVD.Advice(r)</td>
<td>{nvdr \in NVD \mid \exists a \in ADV : r \in R_{nvdr} \land \exists a \in refs_{nvdr}}</td>
</tr>
<tr>
<td>NVD.NBug(r)</td>
<td>{b \in BUG \mid \exists nvd \in NVD : r \in R_{nvd} \land \exists b \in refs_{nvd}}</td>
</tr>
<tr>
<td>Advice.NBug(r)</td>
<td>{b \in BUG \mid \exists a \in ADV : \exists nvd \in NVD : r \in R_{nvd} \land \exists a \in refs_{nvd} \land \exists 1\leq \tau_{nvd} \leq \tau_{max}}</td>
</tr>
</tbody>
</table>

Note: R_{med}, refs_{nvdr} denote the vulnerable releases and references of an entry nvdr, respectively. id_{a}, id_{b}, id_{nvd} denote the identifier of a, b, and nvd. cluster_{s}(id_{a}, id_{nvd}) is a predicate checking whether id_{a} and id_{nvd} are located next together in the advisory.

- NVD.Advice(r): a set of CVEs confirmed by at least a vendor advisory, and claiming r is vulnerable. Notice that the advisory report might not mention r, but later releases.
- NVD.NBug(r): a set of vendor bug reports confirmed by a CVE claiming r is vulnerable.
- Advice.NBug(r): a set of bug reports mentioned in a vendor advisory report, which also refers to at least a CVE that claims r is vulnerable.

We do not use the NVD alone in our studies. We have shown in [31] that it may contain significant errors to the point of tilting statistical conclusions.

An observed sample is a time series of (monthly) cumulative vulnerabilities of a release. It starts from the first month since release to a month specified by the experimenter. This time interval is the horizon of the sample. A month is an appropriate granularity for sampling because week and day are too short intervals and are subject to random fluctuation. Additionally, this granularity was the same granularity reported by all studies listed in TABLE 2.

Let R be the set of analyzed releases and DS be the set of data sets, an observed sample (denoted as os) is a time series (TS) defined as follows:

\[ os = TS(r, ds, \tau) \] (1)

r \in R is a release in the dataset; 
ds \in DS is the data set where samples are extracted;  
\tau \in T_{r} = [\tau_{min}, \tau_{max}] is the horizon of the observed sample, in which T_{r} is the horizon range of release r.

In the horizon range of release r, the minimum value of horizon \( \tau_{min} \) of r depends on the starting time of the first observed sample of r. Here we choose \( \tau_{min} = 6 \) for all releases so that all observed samples have enough data points to achieve statistical applicability of the fitting test. The maximum value of horizon \( \tau_{max} \) depends on the data collection period.

Example 6  IE v4.0 was released in September, 1997 [45]. The first month was October, 1997. The first observed sample of IE v4.0 is a time series of 6 numbers of cumulative vulnerabilities for the 1st, 2nd, . . . , 6th months. On 30th June 2012, IE v4.0 had been released for 182 months, yielding 177 observed samples. The maximum value of horizon (\( \tau_{max}^{IEv4.0} \)) is 182.

4.2  Step 2: Fit a VDM to Observed Samples

We estimate the parameters of the VDM formula by a regression method. The fitted curve (or fitted model) is

\[ vdm_{TS(r, ds, \tau)} = \frac{\sum_{t=1}^{\tau} (O_t - E_t)^2}{E_t} \] (2)

where vdm is the VDM being fitted; os = TS(r, ds, \tau) is an observed sample from which the vdm’s parameters are estimated. (2) could be shortly written as vdm_{os}.

Example 7  Fitting the AML model to the NVD data set of Firefox v3.0 at the 30th month, i.e., the observed sample os = TS(FF3.0, NVD, 30), generates the curve:

\[ AML_{TS(FF3.0, NVD, 30)} = \frac{183}{183 \cdot 0.078 \cdot e^{-0.00183 \cdot t} + 1} \]

Fig. 3 illustrates the plots of three curves AML_{TS(r, NVD, 30)} where r is FF3.0, FF2.0, and FF1.0.

To measure the goodness-of-fit, we employ Pearson’s Chi-Square (\( \chi^2 \)) and calculate the \( \chi^2 \) statistic value of the curve by using the following formula:

\[ \chi^2 = \sum_{t=1}^{\tau} \frac{(O_t - E_t)^2}{E_t} \] (3)

where \( O_t \) is the observed cumulative number of vulnerabilities at time t (i.e., \( t^{th} \) value of the observed sample); \( E_t \) denotes the expected cumulative number of vulnerabilities (the value of the curve at time t). The larger \( \chi^2 \), the smaller goodness-of-fit. If the \( \chi^2 \) value is large enough, we can safely reject the model. The \( \chi^2 \) test requires all expected values be at least 5 to ensure the validity of the test [33, Chap. 1].

The conclusion whether a VDM curve statistically fits an observed sample relies on the \( p-value \) of the test, which is derived from \( \chi^2 \) value and the degrees of freedom (i.e., the number of months minus one). The \( p-value \) is the probability that we wrongly reject the null hypothesis when it is true (i.e., error Type I). The null hypothesis used in past research papers is that “the model fits the data.” [7, page 225]. Therefore, if the \( p-value \) is less than the significance level \( \alpha \) of 0.05, we can reject a VDM because there are less than 5% chances that this fitted model would generate the observed sample. This provides us a robust test to discard a model.

To consider acceptable a VDM, we use as a threshold the power of the \( \chi^2 \) test, the probability of rejecting the null hypothesis when it is indeed false (the complementary of the probability of committing a Type II error). Normally, ‘an 80% power is considered desirable’ [24, Chap. 8]. Hence we accept a VDM if the \( p-value \) is greater than or equal to 0.80, we have more than 80% chances of generating the observed sample from the fitted curve. In all other cases, we neither accept nor reject the model (inconclusive fit). The criteria CR2 in TABLE 4 summarizes the assessment based on the \( p-value \) of the \( \chi^2 \) test.
In the sequel, we use the term evaluated sample to denote the tripod composed of an observed sample, a fitted model, and the p-value of the χ² test.

**Example 8** In Fig. 3, the first plot shows the AML model with a Good Fit (p-value = 0.993 > 0.80), the second plot exhibits the AML model with an Inconclusive Fit (0.05 < p-value = 0.417 < 0.80), and the last one denotes the AML model with a Not Fit (p-value = 0.0001 < 0.05). To calculate the χ² test we refit the model every time.

### 4.3 Step 3: Goodness-of-Fit Quality Analysis

We introduce the goodness-of-fit quality (or quality, shortly) by measuring the overall number of Good Fits and Inconclusive Fits among different samples. Let \( OS = \{TS(r, ds, τ)|r \in R \land ds \in DS \land τ \in T_r\} \) be the set of observed samples, the overall quality of a model \( vdm \) is the weighted ratio of the number of Good Fit and Inconclusive Fit evaluated samples over the total ones:

\[
Q_\omega = \frac{|GES| + \omega \cdot |IES|}{|ES|} \tag{4}
\]

\( ES = \{\langle os, vdm_{os}, p\rangle | os \in OS\} \) is the set of evaluated samples generated by fitting \( vdm \) to observed samples; \( GES = \{\langle os, vdm_{os}, p\rangle \in ES | p \geq 0.80\} \) is the set of Good Fit evaluated samples; \( IES = \{\langle os, vdm_{os}, p\rangle \in ES | 0.05 \leq p < 0.80\} \) is the set of Inconclusive Fit evaluated samples; \( \omega \in [0,1] \) is the inconclusiveness contribution factor denoting that an Inconclusive Fit is \( \omega \) times less important than a Good Fit.

The overall quality metric ranges between 0 and 1. The quality of 0 indicates a completely inappropriate model, whereas the quality of 1 indicates a perfect model. Once again, this metric is an optimistic measure because we are “refitting” the model as more data become available.

The factor \( \omega \) denotes the contribution of an inconclusive fit to the overall quality. A skeptical analyst would set \( \omega = 0\): only Good Fits are meaningful. An optimistic analyst could chose \( \omega = 1\): an Inconclusive Fit is as good as a Good Fit. The optimistic choice \( \omega = 1 \) has been adopted by all model proponents.

The value of \( \omega \) could also be set based on the average p-value \( \bar{p} \) of inconclusive cases.

- If \( \bar{p} \approx 0.05 \), the VDM most likely does not fit the actual data, \( \omega = 0 \).
- If \( \bar{p} \approx 0.80 \), most likely the VDM fits the data, \( \omega = 1 \).

Therefore, we could approximate \( \omega \) as follows:

\[
\omega \approx \frac{\bar{p} - 0.05}{0.80 - 0.05} \tag{5}
\]

where \( \bar{p} \) is the average p-value of inconclusive evaluated samples. We have analyzed about 6, 100 inconclusively evaluated samples, the average p-value: \( \bar{p} = 0.422 \). Replacing this value in (5), we obtain \( \omega \approx 0.5 \). It is consistent with the intuition that an Inconclusive Fit is as half-good as a Good Fit.

**Example 9** Among 3, 895 evaluated samples of AML for IE, Firefox, Chrome, and Safari, AML has 1, 526 Good Fits, 1, 463 Inconclusive Fits. The overall quality of AML with different \( \omega \) thus is: \( Q_{\omega=0} = 0.39, Q_{\omega=0.5} = 1.526 + 0.5 \cdot 1.463 \cdot 1.526 + 0.5 \cdot 1.463 = 0.58, Q_{\omega=1} = 0.77 \).

The overall quality metric does not capture alternating performance in time. A VDM could produce a lot of Good Fits evaluated samples for the first 6 months, but almost Not Fits at other horizons.

To capture this effect, we introduce the temporal quality metric which represents the evolution of the overall quality over time. The temporal quality \( Q_\omega(τ) \) is a function that return the weighted ratio of the Good Fit and Inconclusive Fit evaluated samples over total sample.
Fig. 4. Temporal quality of AML and AT models.

for each value of the horizon \( \tau \).

\[
Q_\omega(\tau) = \frac{\left(\langle GES(\tau)\rangle + \omega \cdot |IES(\tau)|\right)}{|ES(\tau)|}
\]  
\[
(6)
\]

\( \tau \in T \) is the horizon that we observe samples, in which \( T \subseteq \bigcup_{r \in R} T_r \) is the subset of the union of the horizon ranges of all releases \( r \) in evaluation;

\( ES(\tau) = \{<os, vdm_{os}, p> | os \in OS(\tau)\} \) is the set of evaluated samples at the horizon \( \tau \); where \( OS(\tau) \) is the set of observed samples at the horizon \( \tau \) of all releases;

\( GES(\tau) \subseteq ES(\tau) \) is the set of Good Fit evaluated samples at the horizon \( \tau \); 

\( IES(\tau) \subseteq ES(\tau) \) is the set of Inconclusive Fit evaluated samples at the horizon \( \tau \); 

\( \omega \) is the same value used for the overall quality \( Q_\omega \).

To study the trend of the temporal quality \( Q_\omega(\tau) \), we use the moving average to smooth out short-term fluctuations. Each point in the moving average is the average of adjacent points in the original series.

\[
MA_k^Q_\omega(\tau) = \frac{1}{k} \sum_{i=1}^{k} Q_\omega(\tau - i + 1)
\]  
\[
(7)
\]

where \( k \) is the window size. The value \( k \) is less than the minimum horizon \( (k \leq \tau_{\text{min}}) \) for the computation to be possible. Additionally, \( k \) should be an odd number so that variations in the mean are aligned with variations in the data rather than being shifted in time.

Example 10 The moving average in the data rather than being shifted in time.

4.4 Step 4: Perform Predictability Analysis

The predictability of a VDM measures the capability of predicting future trends of vulnerabilities, i.e., its practical relevance. The calculation of the predictability of a VDM has two phases, learning phase and prediction phase. In the learning phase, we fit a VDM to an observed sample at a certain horizon. In the prediction phase, we evaluate the qualities of the fitted model on observed samples in future horizons.

Let \( vdm_{TS(\tau,\delta,\tau)} \) be a fitted model at horizon \( \tau \). The predictability of this model in the next \( \delta \) months (after \( \tau \)) is calculated as follows:

\[
Q_\omega^*(\tau, \delta) = \frac{|GES^*(\tau, \delta)| + \omega \cdot |IES^*(\tau, \delta)|}{|ES^*(\tau, \delta)|}
\]  
\[
(8)
\]

\( ES^*(\tau, \delta) = \{<TS(\tau, ds, \tau + \delta), vdm_{TS(\tau, ds, \tau)}, p>\} \) is the set of evaluated samples at the horizon \( \tau + \delta \) in which we evaluate the quality of the model fitted at horizon \( \tau \)

\( \tau + \delta \). We refer to \( ES^*(\tau, \delta) \) as set of evaluated samples of prediction;

\( GES^*(\tau, \delta) \subseteq ES^*(\tau, \delta) \) is the set of Good Fit evaluated samples of prediction at the horizon \( \tau + \delta \); 

\( IES^*(\tau, \delta) \subseteq ES^*(\tau, \delta) \) is the set of Inconclusive Fit evaluated samples of prediction at the horizon \( \tau + \delta \).

\( \omega \) is the same as for the overall quality \( Q_{\omega} \).

Example 11 Fig. 5 shows the predictability of two models AML and AT starting from the horizon of 12th month (\( \tau = 12 \), left) and 24th month (\( \tau = 24 \), right), and predicting the value for next 12 months (\( \delta = 0 \cdots 12 \)).

In planning, the idea of 3-6-12-24 month rolling plans has been widely adopted in many fields such as banking, clinical trials, and economic planning. We report the predictability of VDMs in next 3, 6, and 12 months, but not in next 24 months because all VDMs perform badly. Assume a new version is shipped every quarter, we could envisage the following illustrative scenarios:

- **Short-term planning** (3 months): we want to predict the trend in the next quarter to allocate resources for fixing vulnerabilities.
- **Medium-term planning** (6 months): we are looking at the next 6 months to decide whether keeping the current system or updating it.
- **Long-term planning** (12 months): we would like to predict vulnerability reports to decide whether to select the software for inclusion in a product with a longer lifetime.

We assess the predictability of a VDM not only along the prediction time span, but also along the horizon to ensure the VDM is able to consistently predict the vulnerability trend in a desired period. For this purpose we introduce the predictability metric which is the average of prediction qualities at a given horizon.

The predictability of the curve \( vdm_{os} \) at the horizon \( \tau \) in a time span of \( \Delta \) months is defined as the average of the predictability of \( vdm_{os} \) at the horizon \( \tau \) and its \( \Delta \) consecutive horizons \( \tau + 1, \tau + 2, \ldots, \tau + \Delta \), as follows:

\[
Predict_{\omega}(\tau, \Delta) = \frac{1}{\Delta} \sum_{\delta=0}^{\Delta-1} Q_{\omega}^*(\tau, \delta)
\]  
\[
(9)
\]
Fig. 5. The prediction qualities of AML and AT.

where $\Delta$ is the prediction time span. We use the geometric mean instead of the arithmetic mean because the temporal quality is a normalized measure [14].

4.5 Step 5: Compare VDMs

This section addresses the second research question RQ2 concerning the comparison between VDMs based on quality and predictability.

VDMs only make sense if they could predict the future trend of vulnerabilities. Hence a VDM which perfectly fits the historical data, but badly estimates the future trend even in a short period, is utterly useless: a better model is the one that better forecasts the future.

The comparison between two models $vdm_1$ and $vdm_2$ is done as follows. Let $\rho_1, \rho_2$ be the predictability of $vdm_1$ and $vdm_2$, respectively.

$$
\rho_1 = \{ \text{Predict}_{\omega=0.5}(\tau, \Delta) \mid \tau = 6..\tau_{\text{max}}, vdm_1 \}
$$

$$
\rho_2 = \{ \text{Predict}_{\omega=0.5}(\tau, \Delta) \mid \tau = 6..\tau_{\text{max}}, vdm_2 \}
$$

(10)

where the prediction time span $\Delta$ could follow the criteria CR4; $\tau_{\text{max}} = \min(72, \max_{r \in R} r^{\tau})$. We employ the one-sided Wilcoxon rank-sum test to compare $\rho_1, \rho_2$. If the returned $p$-value is less than the significance level $\alpha = 0.05$, the predictability of $vdm_1$ is statistically greater than that of $vdm_2$. It also means that $vdm_1$ is better than $vdm_2$. If $p$-value $\geq 1 - \alpha$, we conclude the opposite i.e., $vdm_2$ is better than $vdm_1$. Otherwise we have not enough evidence either way.

If the previous comparison is inconclusive, we repeat the comparison using the value of temporal quality of the VDMs instead of predictability. We just replace $Q_{\omega=0.5}(\tau)$ for $\text{Predict}_{\omega=0.5}(\tau, \Delta)$ in the equation (10), and repeat the above activities.

To compare models, we run several hypothesis tests. To avoid the family-wise error rate, which is the probability of making one or more type I errors by chance, we apply the Bonferroni correction: the significance level is divided by the number of tests performed.

Example 12 When we compare one model against other seven models, the Bonferroni-corrected signifi-

The above comparison activities are summarized in the criteria CR5 (see TABLE 4).

5 Vulnerability Data Infrastructure

This section describes the software infrastructure and the data sources used to compute and maintain our vulnerability warehouse. TABLE 6 presents the vulnerability data sources for the browsers in our study.

5.1 Software Infrastructure

Fig. 6 reports the software infrastructure for collecting vulnerability data of browsers. The infrastructure consists of three layers (separated in panels in the figure):

- **Layer 1: Data Collector** includes a Web Crawler that downloads HTML/XML files from the servers of data providers. These files are piped to the HTML/XML Data Extractor to extract interesting data features (Section 4.1). Missing features in some data sources (e.g., version data in MFSA) are obtained by correlating across data sources by the Data Correlator via the refs feature [23].

- **Layer 2: Data Sampler** extracts observed samples ((1) from Section 4.1).

- **Layer 3: Data Analysis** includes the VDM Model Fitting processor and the VDM Quality/Predictability Analysis processor. The former takes the output of Layer 2 and performs model fitting for all data samples to all VDMs. The output is a collection of evaluated samples. The latter processor takes the generated evaluated samples and executes the quality, predictability analysis (see Step 3, Step 4). It also executes the VDMs comparison (Step 5).

To enable the reproducibility of the experiment, we do not apply any manual sanitizer to the data collection.

5.2 Collected Vulnerability Data Sets

TABLE 7 reports the descriptive statistics of observed samples in five collected data sets described in TABLE 5. The examined browsers have a very different release cycle. Chrome has a very short cycle (about a month), while other browsers have a longer one in our study. This could explain why the means and standard deviations of Chrome are lower than those of other browsers.
Fig. 6. The data processing infrastructure.

The latest time horizon for these data sets is 30th June 2012. We selected these major releases because they were at least one year old in the market at the time of the data collection. The rationale is that some VDMs only work for lifetimes of over a a year, as they explicitly try to model the loss of interest by the attacker. For example, Firefox versions 6 through 14 were released before the end date of June 2012, but were not included: not enough data points. In total, we have collected 4,507 observed samples for 30 major releases of browsers i.e., Chrome v1.0–v12.0, Firefox v1.0–v5.0, IE v4.0–v9.0, and Safari v1.0–v5.0.

6 AN ASSESSMENT ON EXISTING VDMs

We apply the methodology to assess the performance of eight existing VDMs (see also TABLE 8). In this assessment, we consider 8 out of 10 VDMs listed in the taxonomy (see Fig. 1). Two models MVDM and Effect-based AML (AML-E) are excluded. MVDM by Kim et al.[19] require additional data beyond the scope of this study, i.e., the ratio of share code between versions, which is only available for Chrome and Firefox, though Kim et al. offered an explanation for the deviation from the logistic shape. AML-E [2] uses the test-effort as the main factor instead of the calendar time, which is not comparable to other models.

We follow Step 2 to fit the above VDMs to collected observed samples. The model fitting relies on the function nls() of R [37]. The model fitting took approximately 82 minutes on a dual-core 2.73GHz Windows machine with 6GB of RAM yielding 31, 241 curves in total. During the model fitting, nls() is unable to fit some models in some observed samples. Hence the number of generated curves are less than the number of observed samples multiplied by the number of VDMs.

TABLE 7
Descriptive statistics of observed data samples

<table>
<thead>
<tr>
<th>Browser Releases</th>
<th>NVD</th>
<th>NVD.Bug</th>
<th>NVD.Advice</th>
<th>NVD.NBug</th>
<th>Advice.NBug</th>
<th>All Data Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>8</td>
<td>378</td>
<td>42 47 30</td>
<td>378</td>
<td>42 47 30</td>
<td>378 42 47 30</td>
</tr>
<tr>
<td>Chrome</td>
<td>12</td>
<td>281</td>
<td>20 23 10</td>
<td>281</td>
<td>20 23 10</td>
<td>281 20 23 10</td>
</tr>
<tr>
<td>IE</td>
<td>5</td>
<td>573</td>
<td>130 115 59</td>
<td>573</td>
<td>130 115 59</td>
<td>573 130 115 59</td>
</tr>
<tr>
<td>Safari</td>
<td>5</td>
<td>314</td>
<td>60 63 35</td>
<td>314</td>
<td>60 63 35</td>
<td>314 60 63 35</td>
</tr>
<tr>
<td>Total</td>
<td>30</td>
<td>1,546</td>
<td>36 52 44</td>
<td>659</td>
<td>27 33 23</td>
<td>378 42 47 30</td>
</tr>
</tbody>
</table>

Note: erf() is the error function, erf(x) = \( \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \)

TABLE 8
The VDMs in evaluation and their equation.

VDMs are listed in the alphabetical order. The meaning of the VDMs' parameters are referred to their original work.

<table>
<thead>
<tr>
<th>Model</th>
<th>Equation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alhazmi-Malaiya Logistic (AML) [6]</td>
<td>( \Omega(t) = \frac{B}{Be^{-At} + 1} )</td>
</tr>
<tr>
<td>Anderson Thermodynamic (AT) [8]</td>
<td>( \Omega(t) = \frac{b}{\ln(t) + C} )</td>
</tr>
<tr>
<td>Joh Weibull (JW) [18]</td>
<td>( \Omega(t) = \gamma(1 - e^{-\left(\frac{t}{\beta}\right)^\alpha}) )</td>
</tr>
<tr>
<td>Linear (LN)</td>
<td>( \Omega(t) = At + B )</td>
</tr>
<tr>
<td>Logistic Poisson (LP) [26]</td>
<td>( \Omega(t) = \beta_0 \ln(1 + \beta_1 t) )</td>
</tr>
<tr>
<td>Rescorla Exponential (RE) [39]</td>
<td>( \Omega(t) = N(1 - e^{-\lambda t}) )</td>
</tr>
<tr>
<td>Rescorla Quadratic (RQ) [39]</td>
<td>( \Omega(t) = \frac{At^2}{1 + Bt} )</td>
</tr>
<tr>
<td>Younis Folded (YF) [53]</td>
<td>( \Omega(t) = 2 \cdot \frac{\beta x}{\gamma} \left[ \text{erf} \left( \frac{t - \tau}{\sqrt{\beta \gamma}} \right) + \text{erf} \left( \frac{t + \tau}{\sqrt{\beta \gamma}} \right) \right] )</td>
</tr>
</tbody>
</table>

Note: \( \text{erf}(x) \) is the error function, \( \text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \)

82 minutes on a dual-core 2.73GHz Windows machine with 6GB of RAM yielding 31, 241 curves in total. During the model fitting, nls() is unable to fit some models in some observed samples. Hence the number of generated curves are less than the number of observed samples multiplied by the number of VDMs.
Fig. 7. The trend of temporal quality $Q_{w=0.5}(τ)$ of the VDMs in first 72 months.

Table 9: Overall distribution of evaluated samples.

<table>
<thead>
<tr>
<th>Model</th>
<th>NVD</th>
<th>NVD.Bug</th>
<th>NVD.Advice</th>
<th>NVD.NBug</th>
<th>Advice.NBug</th>
<th>All Data Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>G.F</td>
<td>I.F</td>
<td>N.F</td>
<td>Total</td>
<td>G.F</td>
</tr>
<tr>
<td>AML</td>
<td>1,375</td>
<td>43%</td>
<td>32%</td>
<td>24%</td>
<td>559</td>
<td>30%</td>
</tr>
<tr>
<td>AT</td>
<td>1,378</td>
<td>8%</td>
<td>18%</td>
<td>74%</td>
<td>559</td>
<td>10%</td>
</tr>
<tr>
<td>JW</td>
<td>1,344</td>
<td>38%</td>
<td>18%</td>
<td>44%</td>
<td>547</td>
<td>28%</td>
</tr>
<tr>
<td>LN</td>
<td>1,378</td>
<td>36%</td>
<td>19%</td>
<td>45%</td>
<td>559</td>
<td>20%</td>
</tr>
<tr>
<td>LF</td>
<td>1,377</td>
<td>42%</td>
<td>14%</td>
<td>43%</td>
<td>559</td>
<td>19%</td>
</tr>
<tr>
<td>RE</td>
<td>1,378</td>
<td>41%</td>
<td>14%</td>
<td>44%</td>
<td>559</td>
<td>20%</td>
</tr>
<tr>
<td>RQ</td>
<td>1,378</td>
<td>29%</td>
<td>20%</td>
<td>51%</td>
<td>559</td>
<td>24%</td>
</tr>
<tr>
<td>YF</td>
<td>1,358</td>
<td>55%</td>
<td>20%</td>
<td>25%</td>
<td>551</td>
<td>54%</td>
</tr>
<tr>
<td>Total</td>
<td>10,966</td>
<td>37%</td>
<td>19%</td>
<td>44%</td>
<td>4,452</td>
<td>26%</td>
</tr>
</tbody>
</table>

The X-axis is the number of months since release (i.e., horizon $τ$). The Y-axis is the value of temporal quality. The solid lines are the moving average of $Q_{w=0.5}(τ)$ with window size $k = 5$. The dotted horizontal line at 0.5 is the base line to assess VDM. Vertical lines are the marks of the horizons of 12th and 36th month.

In summary, our quality analysis shows that:

- AT and RQ models should be rejected.
- All other models may be adequate when browser is young. Only s-shape models (i.e., AML, YW, YF) might be adequate when browsers are middle-age.
- No model is good enough when browsers are old.

6.2 Predictability Analysis for VDMs

From the previous quality analysis, AT and RQ models are low quality. Hence, we exclude these models from the predictability analysis. Furthermore, since no model is good when browsers are too old, we analyze the predictability of these models only for the first 36 months from a release date. This period is still large as recent releases live less than a year [12, 44, 45, 46].

Predictability is a bi-dimensional function as it takes the horizon of data collection for fitting and the predictability analysis.
6.3 Comparison of VDMs

The comparison between VDMs follows Step 5. Instead of reporting tables of p-values, we visualize the comparison results in terms of directed graphs where nodes represent models, and connections represent the order relationship between models.

Fig. 9 summarizes comparison results between models for different horizons (τ) and prediction time spans (Δ) along the following convention:

- **Solid line**: predictability and quality of the source is significantly better than the target’s.
- **Dashed line**: predictability of the source is significantly better than the target.
- **Dotted line**: quality of the source is significantly better than the target.

By the word *significantly*, we mean the *p-value* of the corresponding one-sided Wilcoxon rank-sum test is less than the significance level. We apply the Bonferroni correction to control the multi comparison problem, hence...
From TABLE 11, we might conclude: (1) AML and YF are the “best” model (YF is slightly better than AML); (2) AT and RQ are the “worst”; and (3) other models are approximately equal.

With reference to TABLE 1 (or TABLE 10), the conclusions obtained by the traditional methodology are clearly less informative than those by our methodology. They both agree that AT and RQ are the worst. However, our methodology provides statistical evidences about the superior performance of LN and AML in different periods of browser lifetime, whereas the traditional one does not.

An interesting issue is whether we need the full complexity of the methodology and could attain the same insight by a reduced number of steps. We could have stopped the analysis at Step 2, after TABLE 9. This table does not distinguish between AML and YF. Moreover, it obfuscates the greater performance of LN for the first year since release. This is a major issue for today’s software whose lifecycle is very short.

In summary, our methodology provides more practical information about the performance of VDMs in different scenarios than the traditional methodology.

### 8 Threats to Validity

Some threats to Construct validity may affect our data. **Bugs in data collector.** The vulnerability data is collected by a crawler parsing HTML pages. It might be buggy. We minimize this threat by randomly checking the data. When an error was found we corrected the crawler and recollected the data.

**Bias in bug-to-nvd linking scheme.** While collecting data for Advice, Nbug, we apply heuristics to link a bug to an NVD entry based on their positions in an MFSA report. We manually checked many links for inconsistencies.

**Bias in bug-affects-version identification.** We do not completely known which bugs affect which versions. We assume that a bug affects all versions mentioned in its linked NVD entry. This might overestimate the number of bugs in each version. So, we estimate the latest release that a bug might impact, and filter all vulnerable releases after this latest. Such estimation is done by the technique discussed in [43], [31]. The potential errors in NVD discussed in [31] only affect the retrospective fitness of models over the long term so only valuations after 36 months might be affected.

**Internal validity** threats affect the causal relationship between the collected data and the conclusion in the study. Our conclusions are based on statistical tests. We analyzed the tests assumptions to make sure no unwarranted assumption was present. We did not apply any tests with normality assumptions since the distribution of vulnerabilities is not normal.

Notably, the collected data sets in TABLE 7 are not independent each others, for instance NVD.Bug and NVD.Advice are sub sets of NVD. They represent for different ways of counting vulnerabilities from the NVD.
data source. We treat these data sets equally and fit them all to VDMs to address the issues behind vulnerability count methods (Section 3). This might have an accumulative effect on quality and predictability. We believe this accumulative effect is negligible because TABLE 9, reporting statistics of evaluated samples, shows that responses of VDMs to different data sets are very different.

Another potential internal validity problem is the ‘independently distributed’ assumption that statistical tests might violate. This could be the case when developers discover a vulnerability, realize they make mistakes elsewhere, and go back to fix other mistakes in the same area of the system. For reported vulnerabilities in Firefox and Chrome, the analysis of the commit logs shows that each fix mostly corresponds to a fix of a single vulnerability, and each fix touches very few components (on average, 1.17 for Firefox, and 1.84 for Chrome [30]). It means the problem is minor in our study, at least for Firefox and Chrome. If mistakes are not reported as vulnerability entries, they do not “exists” for us, and therefore the reported entries are indeed independent (the dependent events are not present at all).

External validity is the extent to which our conclusion could be generalized to other scenarios. Our experiment is based on the four most popular browsers. So we can be confident about our conclusion for browsers in general, but it might not be valid for other types of application such as operating systems. Such validity requires additional experiments.

9 Conclusion

Vulnerability discovery models (VDMs) have the potential to help us in predicting future trends of vulnerabilities, adapting software update and patching schedule, or selecting (open source) products to bundle into other proprietary products.

The major contribution of this work is an empirical methodology to conduct evaluation experiments on VDMs. The quality and predictability of VDMs in question are measured by two functions that report the ability to fit vulnerability data and the ability to predict future vulnerabilities as function of time. As a result, we obtain a better insight about VDMs.

To illustrate the methodology, the paper reports an evaluation experiment to assess eight VDMs (i.e., AML, AT, LN, JW, LP, RE, RQ, and YF) on 30 major releases of four web browsers: IE, Firefox, Chrome, and Safari. We classify the age of a browser’s version in three different periods: youth (within 6 – 12 months since release date), middle age (12 – 36 months since release date), and old age (beyond 36 months). Our experiment reveals interesting findings on these existing VDMs: if a version is relatively young, then we should use a linear model to estimate the vulnerabilities in the next 3 – 6 months. For middle-aged browsers it is better to use an s-shape logistic model. This would have insight been impossible to achieve with the traditional methodology.

A number of further investigations is possible such as replicate the experiment with other software types. We did not consider MVDM model [19] and effort-based models because they require data that is beyond the scope of this study. An interesting issue is understanding whether the speed of the release cycle and/or the size of the releases impacts VDMs quality. Another question is evaluating how errors in the datasets may impact the analysis [31]. Further assessments in these directions will make the understanding of VDMs more comprehensive.

10 Replication Guideline

We have made the data in this work available online. Interested readers who want to reproduce the experiment could obtain the data at http://securitylab.disi.unin.it/.

Acknowledgements

We would like to thank all anonymous reviewers for their helpful comments and suggestion. This work has been partly supported by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 285223 - SECONOMICS, and the Italian Project MIUR-PRIN-TENACE.

References


