Security Vulnerabilities: Risks from Discovery to Exploitation

Yashwant K. Malaiya
Colorado State University
Common Vulnerability Scoring System (CVSS)

- *De facto* industry standard for assessing the severity of computer security vulnerabilities
- Ranges 0.0 ~ 10.0
- Effort could be prioritized
- Consists three metric groups:
  - Base (mandatory) : intrinsic and fundamental
  - Temporal : change over time
  - Environmental : particular user’s environment
CVSS Base metric

Exploitability sub-score

captures how a vulnerability is assessed and whether or not extra conditions are required to exploit it in terms of Access Vector, Access Complexity, and Authentication, each with numerical values in the range [0.0 ~ 10.0]

Impact sub-score

• measures how a vulnerability, if exploited, will directly affect an IT asset in terms of Confidentiality, Integrity, and Availability. [0.0 ~ 10.0]

Base score formula[4]

\[
\text{Base score} = \text{Round to 1 decimal} \left[ 0.6 \times \text{impact} + 0.4 \times \text{exploitability} - 1.5 \right] \\
\times f(\text{impact})
\]

CVSS Base metric: Observation

- **Exploitability sub-score** - measure of Likelihood of exploitation of the vulnerability.
- **Impact sub-score** - a measure of Impact.
- **CVSS Base Score** is a form of a risk measure. They could have computed **CVSS Base Score** by simply multiplying the **Exploitability** and the **Impact sub-scores**. It would result in a similar distribution of score with somewhat better resolution.
- **CVSS Base Score** for prioritizing vulnerabilities. Base score 7.0-10.0 **critical**, 4.0-6.9 **major**, 0-3.9 **minor**.
- The CVSS Base Score formula was determined by a committee and not formally derived or explained.
CVSS and recent Research
Distribution of Base score

<table>
<thead>
<tr>
<th>Min.</th>
<th>1st Qu.</th>
<th>Median</th>
<th>Mean</th>
<th>3rd Qu.</th>
<th>Max.</th>
<th>Combinations</th>
</tr>
</thead>
</table>
| (a)  | 0       | 5      | 6.8    | 6.341   | 7.5  | 10           | 63
| (b)  | 0       | 29     | 49     | 48.59   | 64   | 100          | 112

NVD on Jan 2011 (44615 vuln.)

Has CVSS worked?

- Windows 7 Correlation among
  - CVSS Exploitability
  - Microsoft Exploitability metric
  - Presence of actual exploits
- No significant correlation found.
- Continuing research

<table>
<thead>
<tr>
<th>Variables</th>
<th>Exploit Existence</th>
<th>MS-EXP</th>
<th>CVSS-EXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploit Existence</td>
<td>1</td>
<td>-0.078</td>
<td>-0.146</td>
</tr>
<tr>
<td>MS-EXP</td>
<td>-0.078</td>
<td>1</td>
<td>-0.116</td>
</tr>
<tr>
<td>CVSS-EXP</td>
<td>-0.146</td>
<td>-0.116</td>
<td>1</td>
</tr>
</tbody>
</table>

Likelihood of Individual Vulnerabilities Discovery

- **Ease of discovery**
  - Human factor (skills, time, effort, etc.), Discovery technique, Time

- **Time:**

  - Apache HTTP server
  - CVE-2012-0031, (01/18/2012)
  - V. 1.3.0 → 1998-06-06

**Time to Discovery** = Discovery Time Date – First Effected version Release Date
Correlation: Access complexity vs Time to Discover

- **AC vs Time**
  - **AC = Low**
    
    | Min. | 1st Qu. | Median | Mean | 3rd Qu. | Max. |
    |------|---------|--------|------|---------|------|
    | 0.100| 0.900   | 2.000  | 3.338| 4.500   | 18.000|
  
  - **AC = Medium**
    
    | Min. | 1st Qu. | Median | Mean | 3rd Qu. | Max. |
    |------|---------|--------|------|---------|------|
    | 0.100| 2.000   | 6.500  | 6.819| 9.500   | 18.000|
  
  - **AC = High (very few points)**
    
    | Min. | 1st Qu. | Median | Mean | 3rd Qu. | Max. |
    |------|---------|--------|------|---------|------|
    | 0.400| 1.350   | 3.500  | 5.208| 7.125   | 18.000|

- Some correlation between Access Complexity and Time to Discover
Characterizing Vulnerability with Exploits

- **1 to 5 %** of defects are vulnerabilities.

- Finding vulnerabilities can take considerable expertise and effort.

- Out of 49599 vulnerabilities reported by NVD, **2.10%** have an exploit.

- A vulnerability with an exploit written for it presents more risk.

- **What characterizes a vulnerability having an exploit?**

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>In-Degree</th>
<th>Out-Degree</th>
<th>CountPath</th>
<th>ND</th>
<th>CYC</th>
<th>Fan-In</th>
<th>No of Invocation</th>
<th>SLOC</th>
<th>Exploit Existence</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2009-1891</td>
<td>1</td>
<td>9</td>
<td>9000</td>
<td>6</td>
<td>68</td>
<td>45</td>
<td>2</td>
<td>211</td>
<td>NEE</td>
</tr>
<tr>
<td>CVE-2010-0010</td>
<td>4</td>
<td>9</td>
<td>145</td>
<td>4</td>
<td>11</td>
<td>16</td>
<td>4</td>
<td>38</td>
<td>EE</td>
</tr>
<tr>
<td>CVE-2013-1896</td>
<td>26</td>
<td>5</td>
<td>8</td>
<td>1</td>
<td>5</td>
<td>37</td>
<td>3</td>
<td>29</td>
<td>EE</td>
</tr>
</tbody>
</table>

Vulnerabilities & Money

Attacker

Discovery

Black Market

Exploitation

Attack observed in monitored systems

Security Professional

Discovery

Immediate Disclosure (e.g., Bug Traq)

Nonpublic Disclosure (e.g., CERT)

Market Disclosure (e.g., iDefense)

Vendor

Subscribers

Public Disclosure
Vulnerability flow through markets
Types of Vulnerability Markets

- Freelance Discoverers “Sellers”
- Captive Discoverers

Vulnerability information

- Regulated Market
  - Publicity
  - Captive
  - Reward Programs
  - Security Company
  - Online Forum

- Software Developers “Buyers”
  - Resolve by patches

Producers

Vulnerability Markets

Consumers

Attacks/Resolutions

- Hacktivists
- Government agencies
- Malicious attackers

- Organizations
- Organizations in other countries
- Organization attacks
Vulnerability Reward Programs
There is a significant correlation

<table>
<thead>
<tr>
<th></th>
<th>Correlation</th>
<th>CVSS Scores before clustering</th>
<th>CVSS Scores after clustering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>Value</td>
<td>0.65</td>
<td>0.47</td>
</tr>
<tr>
<td></td>
<td>P-value</td>
<td>&lt; 0.0001</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>Chrome</td>
<td>Value</td>
<td>0.53</td>
<td>0.59</td>
</tr>
<tr>
<td></td>
<td>P-value</td>
<td>&lt; 0.0001</td>
<td>&lt; 0.0001</td>
</tr>
</tbody>
</table>

Vulnerability Reward Programs

• VRPs decreases the probability of an attacker acquiring a vulnerability and that reduces the likelihood of vulnerabilities discovery and exploitation.

• Vulnerabilities with a high CVSS scores and have no exploits or attacks may been explained by the impact of VRPs on vulnerabilities exploitation.
Measuring Impact

- Technical impact in terms of Confidentiality, Integrity, Availability: CVSS Impact factor, not validated
- Methods for computing business impact are still evolving
- Widely different estimates of financial impacts of recent security breaches
- Our effort is continuing
Conclusions

- Risk as Likelihood x Impact product
- Conditional components of Likelihood
- Vulnerability discovery and lifecycle
- CVSS as a risk measure: not validated
- Measuring impact: needs further research
References


