Putting private and government CERT’s to the test

Stefan Frei, Martin May

ETH Zurich: http://www.csg.ethz.ch
Paper download: http://www.techzoom.net/risk
Outline

- We discuss the role of security information providers with respect to today's security ecosystem.
- We identify the most well-known sources where security advisories can be found and present a methodology to measure the performance of these information providers.
Evolution of the Internet society

- Situation
  - Global Internet penetration and e-commerce growths have experienced an explosive increase over the past years.
  - Information technology has become a backbone of our industry and everyday life.
  - The constant discovery, publication and exploitation of new vulnerabilities drives the security risks we are constantly exposed to.
Today's challenge

- **Challenge**
  - Businesses and enterprises need accurate and validated vulnerability information from a trusted source!
  - Many organizations publish information on new vulnerabilities and even more organizations depend on such sources for security information.
  - **What are viable security information sources?**
Sources of Security Information

Requirements
- We want trusted, unbiased and timely security vulnerability information in a standard format.

Security Information Provider (SIP)
- CERT’s and private sector services provide security information through the publication of vulnerability advisories.
  - SIPs monitor the (in)security scene, do research and collaborate with vendors to provide security information to the public.
Security Information Provider (SIP)

- Sources
  - The most referenced sources of security information:
    - **US-CERT**, USA, since 1988
    - **IBM Internet Security Systems X-Force (XF)**, USA, since 1996
    - **SecurityFocus** (SF), USA, since 1996
    - **Secunia**, Denmark, since 2003
    - **FrSIRT**, France, since 2005
    - **SecurityTracker**, USA, since 2001
    - **SecurityWatch**, USA, since 2004
Other Sources

- Exploit archives
  - We also include three well known exploit archives in our study .. to shed a light on the "other side" of the security industry.
  - Milw0rm
  - PacketStorm
  - SecurityVulns

- National Vulnerability Database (NVD)
  - Source for risk rating of vulnerabilities

National Vulnerability Database (NVD) [www.nvd.nist.gov](http://www.nvd.nist.gov)
The role of Security Information Providers
Vulnerability Lifecycle

- Processes & Timing
  - The exact sequence of events varies between vulnerabilities.
  - Different processes are involved in the **discovery**, **exploitation**, **disclosure** and **patching** of vulnerabilities.
# Lifecycle Events

<table>
<thead>
<tr>
<th>Process/Event</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>by whom?</td>
</tr>
<tr>
<td></td>
<td>- the good &gt; report responsibly</td>
</tr>
<tr>
<td></td>
<td>- the bad &gt; misuse, exploit</td>
</tr>
<tr>
<td>Disclosure</td>
<td>by whom?</td>
</tr>
<tr>
<td></td>
<td>- coordinated disclosure?</td>
</tr>
<tr>
<td></td>
<td>- vendor/public taken by surprise?</td>
</tr>
<tr>
<td>Exploitation</td>
<td>through the bad</td>
</tr>
<tr>
<td>Patching</td>
<td>by vendor (originator)</td>
</tr>
<tr>
<td></td>
<td>- when is a patch available?</td>
</tr>
<tr>
<td></td>
<td>- when is it installed?</td>
</tr>
</tbody>
</table>
Important Processes

- Vulnerability first
  - SIPs monitor the (in)security scene, conduct own research, collaborate with vendors.
  - These activities result in security advisories.

- Patch first/coordinated disclosure
  - Patches released by vendors get analyzed by SIPs, resulting in a security advisory.

- Exploit first
  - An exploit in the wild gets analyzed by SIPs, resulting in a security advisory.
Dynamics of (In)Security

- Very high dynamics at the **disclosure date**.
- Exploit (red), Patch (green) dynamics before/after disclosure

![Graph showing dynamics of security](image)

**Exploits quickly result in security advisory by SIPS**

**Information is badly needed till patch is available**

Source: Speed of (In)Security - BlackHat 06 - [www.techzoom.net/publications](http://www.techzoom.net/publications)
Role of Security Information Providers

- **Monitoring**
  - SIPs effectively and efficiently monitor the (in)security scene. New security issues are quickly released as security advisories to the public.

- **Watchdogs**
  - Independent and trusted SIPs act like the free press in an open society: efficient watchdogs to expose important issues to the public!
  - This is an essential role for the well-being and functioning of the security ecosystem.
Methodology & Data Gathering
Methodology

- Methodology
  - Definition of „vulnerability“ and identification of data sources.

- Process phases
  - Monitor the appearance of new advisories/exploits with 30 min intervals since August 2006
  - Download and parse all known advisories from monitored SIPs
  - Correlate the information gained in phases (1) and (2).
What is a vulnerability?

- Definition of a vulnerability
  - Counting or defining vulnerabilities is a delicate business that depends significantly on the parties involved.
  - If something is considered a *bug*, a *feature*, or a *vulnerability* may differ if you talk to a researcher or the vendor of the affected software.
  - Several different definitions exist ...
What is a vulnerability - CVE

- Common Vulnerabilities and Exposures (CVE)
  - A dictionary of common names (identifiers) for publicly known vulnerabilities.
  - A *de facto* industry standard that has achieved wide acceptance in the security industry, academia, and government organizations.
  - CVE is run by MITRE, a non-profit organization of the U.S government chartered to work in the public interest.

Source: [www.cve.mitre.org](http://www.cve.mitre.org)
What is a vulnerability - CVE

- Flow of security information
  - A number of organizations in the security community provide CVE with vulnerability information.
  - Since CVE does not rely on one single source, it has a better chance of identifying all publicly known security problems.
  - This process provides a more comprehensive set of vulnerability information for everyone.

- Building the CVE list
  - Submission (analyze, research, process)
  - Candidate Stage (submissions, reserved, out-of-band)
  - Entry Stage (accepted)
What is a vulnerability - CVE

- CVE provides the security community:
  - A comprehensive list of publicly known vulnerabilities.
  - An analysis of the authenticity of newly published vulnerabilities.
  - A unique identifier for each vulnerability.

- Given the high acceptance of CVE we assume that any security issue of relevance will eventually get an CVE assigned.

- From the original 321 entries in 1999, the CVE list has grown to over 30,000 entries as of April 2008.
CVE Content/SIP Identification (January 1st, 2008)

- 29,797 CVE entries contained 158,779 external references to 77 different sources.
- Sources we cover in this study are marked by (*), covering >50% of the CVEs

<table>
<thead>
<tr>
<th>Source</th>
<th>Referenced</th>
<th>Cumulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secunia (*)</td>
<td>15.36%</td>
<td>15.36%</td>
</tr>
<tr>
<td>SecurityFocus (*)</td>
<td>13.08%</td>
<td>28.44%</td>
</tr>
<tr>
<td>IBM ISS X-Force (*)</td>
<td>12.36%</td>
<td>40.80%</td>
</tr>
<tr>
<td>BugTraq</td>
<td>11.23%</td>
<td>52.03%</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>6.50%</td>
<td>58.53%</td>
</tr>
<tr>
<td>FrSIRT (*)</td>
<td>6.47%</td>
<td>65.00%</td>
</tr>
<tr>
<td>OSVDB</td>
<td>5.29%</td>
<td>70.29%</td>
</tr>
<tr>
<td>SecurityTracker (*)</td>
<td>4.05%</td>
<td>74.34%</td>
</tr>
<tr>
<td>Sreason</td>
<td>2.46%</td>
<td>76.80%</td>
</tr>
<tr>
<td>CERT (*)</td>
<td>2.28%</td>
<td>79.08%</td>
</tr>
</tbody>
</table>
Correlation

- Correlation
  - Download and parse security advisories and exploits advisories in observation period.
  - We used CVE identifiers to correlate security advisories among different sources.
  - We used references (\(=URLs\)) in security advisories, NVD and CVE documents to correlate advisories and/or exploits.
Measurements
Advisories by Source

<table>
<thead>
<tr>
<th>Source</th>
<th>2007</th>
<th>2006</th>
<th>2005</th>
<th>2004</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISS</td>
<td>6,022</td>
<td>6,672</td>
<td>4,401</td>
<td>2,600</td>
</tr>
<tr>
<td>SF</td>
<td>4,797</td>
<td>5,386</td>
<td>3,302</td>
<td>2,303</td>
</tr>
<tr>
<td>Secunia</td>
<td>4,535</td>
<td>5,754</td>
<td>4,022</td>
<td>2,063</td>
</tr>
<tr>
<td>FrSIRT</td>
<td>3,842</td>
<td>5,019</td>
<td>2,282</td>
<td>-</td>
</tr>
<tr>
<td>SecTrack</td>
<td>1,665</td>
<td>2,162</td>
<td>1,840</td>
<td>1,488</td>
</tr>
<tr>
<td>SecWatch</td>
<td>1,098</td>
<td>1,126</td>
<td>1,216</td>
<td>429</td>
</tr>
<tr>
<td>CERT</td>
<td>330</td>
<td>480</td>
<td>299</td>
<td>321</td>
</tr>
<tr>
<td>NVD</td>
<td>6,532</td>
<td>6,600</td>
<td>4,928</td>
<td>2,450</td>
</tr>
</tbody>
</table>

- Number of **unique CVEs** covered by advisories of different sources.
- 6,532 (=100%) vulnerabilities were published in 2007 (based on the NVD publication date)
## Coverage by Source - 2007

<table>
<thead>
<tr>
<th>Source</th>
<th>% ISS</th>
<th>SF</th>
<th>Secunia</th>
<th>FrSIRT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISS</td>
<td>6,022</td>
<td>6.264</td>
<td>6,437</td>
<td>6,416</td>
</tr>
<tr>
<td></td>
<td>92%</td>
<td>95%</td>
<td>99%</td>
<td>98%</td>
</tr>
<tr>
<td>SF</td>
<td>4,797</td>
<td>5,802</td>
<td>5,637</td>
<td></td>
</tr>
<tr>
<td></td>
<td>73%</td>
<td>89%</td>
<td>86%</td>
<td></td>
</tr>
<tr>
<td>Secunia</td>
<td></td>
<td>4,535</td>
<td>5,042</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>69%</td>
<td>77%</td>
<td></td>
</tr>
<tr>
<td>FrSirt</td>
<td></td>
<td></td>
<td>3,842</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>59%</td>
<td></td>
</tr>
</tbody>
</table>

- Best coverage from single source: 92%.
- When any two SIP are combined we get between 95% to 99% coverage.
- **We want multiple independent SIPs!**
Publication Dynamics

- **Publication timing**
  - We look at the distribution of advisory and exploit publications:
    - by the hour during the day.
    - by the weekday during the week.

- **Performance Comparison**
  - We examine the timing of the publication of security advisories between the sources.
By the hour of the day

All times UTC
- SIPs
- Exploits
By the hour of the day

Time zones
- Americas
- Europe
- Far East

Automated Tools?

All times UTC
- SIPs
- Exploits
By the day of the week

SIPS (the good):
low weekend activity

Exploits (the bad):
uniform activity throughout the week

All times UTC
- SIPS
- Exploits
Performance Comparison

- Timing of Security Advisory publications
  - We examine the timing of security advisory publications between SIPs.
  - For all CVEs published in 2007, we noted the time of disclosure of each SIP. The majority of CVEs were covered by more than one SIP.
  - We then evaluate the time the first advisory was published and the delay of all other SIPs.
Performance Comparison (0-48h)

Percentage of advisories disclosed by a given source within time $t$ after the first disclosure.
Results

- Generally, we observe high dynamics in the 24h after the first publication.

- Secunia is in 48% of the vulnerabilities the first SIP to disclose, closely followed by SecurityFocus 45%.

- At 24h, SecurityFocus and IBM-ISS lead with about 85%, closely followed by SecTrack and Secunia at about 80%.

- Note that the first publication of a vulnerability can be attributed to more than one SIP at the same time when published simultaneously.
Results

- All but one SIP are first contributors and there is no single source everyone else copies from.

- We further found that the risk rating of a vulnerability does not affect the timeliness of disclosure.
Conclusion
Conclusion

- We observe a healthy and highly competitive market between the different security information providers.
- This market ensures that the public has access to timely and accurate security information.
- This diversity and choice of source is preferred over a single (government sponsored) agency providing security information.
- We want many competing SIPs and CERTs!
Contact

Stefan Frei
frei@techzoom.net

Paper Download: www.techzoom.net/risk

Research sponsored by

\[\text{ETH} \]
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

\textbf{Swiss Federal Institute of Technology, Zurich}
www.csg.ethz.ch