



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



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?**
The vendor? Security mailing lists? Government CERTs? Private enterprises?



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



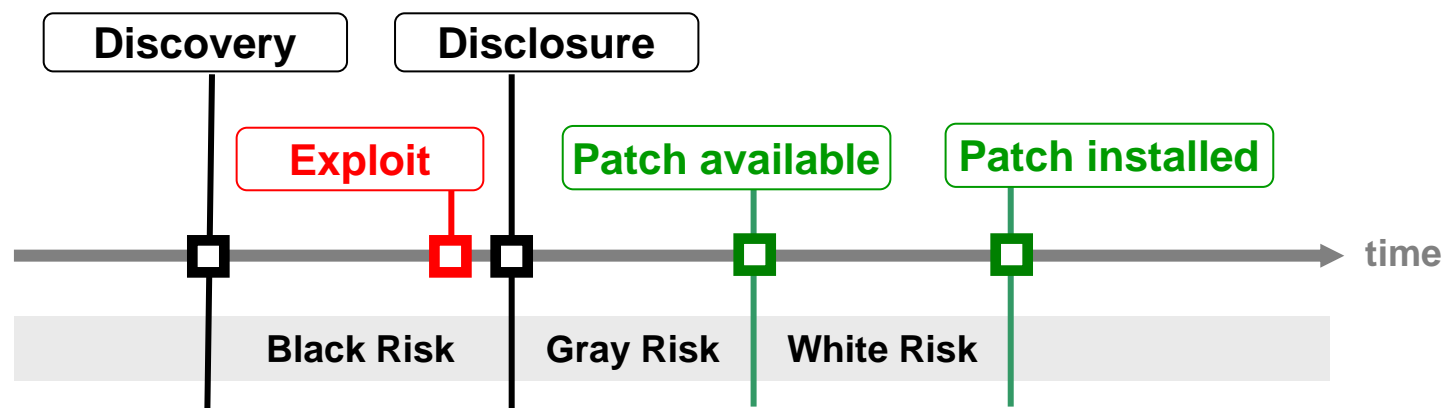
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



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

| Process/Event | Remarks |
|-----------------------|---|
| ▪ Discovery | by whom? <ul style="list-style-type: none">▪ the good > report responsibly▪ the bad > misuse, exploit |
| ▪ Disclosure | by whom? <ul style="list-style-type: none">▪ coordinated disclosure?▪ vendor/public taken by surprise? |
| ▪ Exploitation | through the bad |
| ▪ Patching | by vendor (originator) <ul style="list-style-type: none">▪ when is a patch available?▪ when is it installed? |



Important Processes

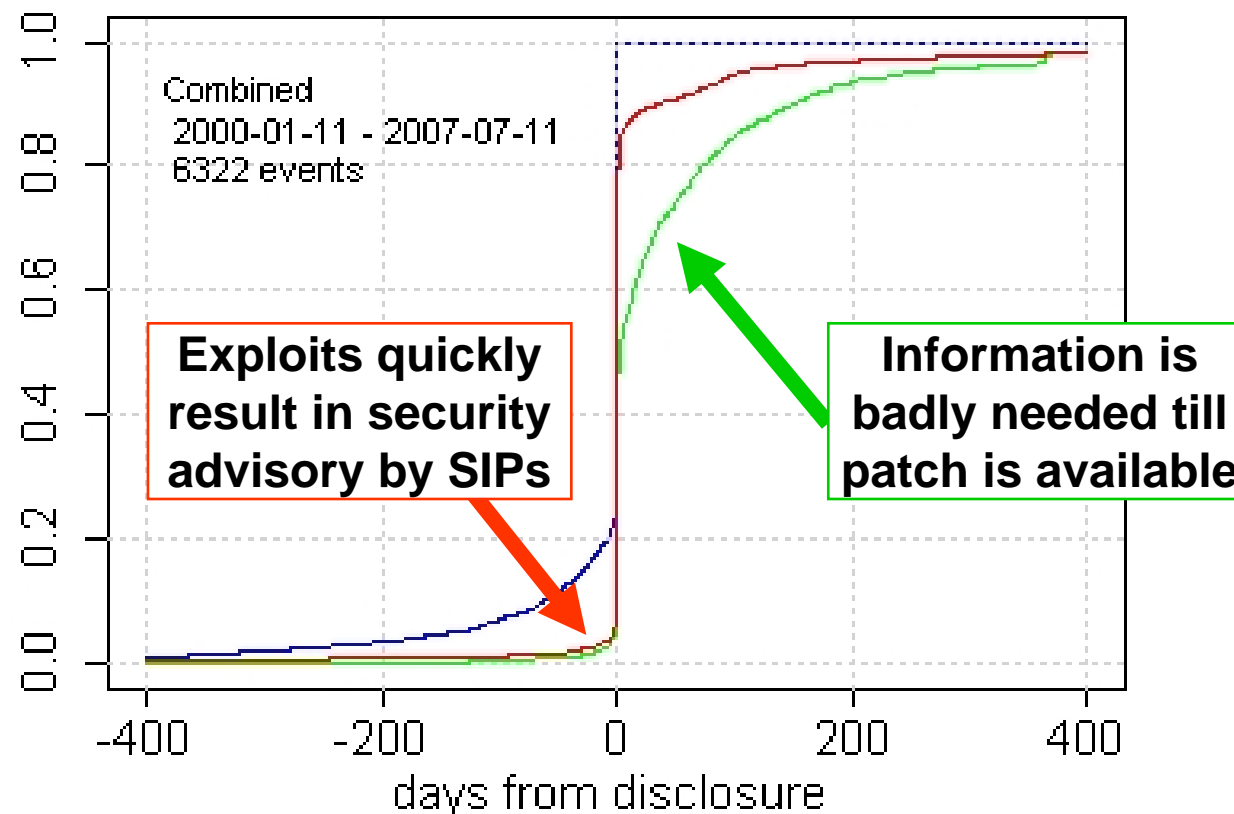
- Vulnerability first
 - SIPs monitor the (in)security scene, conduct own research, collaborate with vendors.
 - These activities result in security advisories.

- 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



Source: Speed of (In)Security - BlackHat 06 - 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.



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



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



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

| Source | Referenced | Cumulated |
|---------------------|------------|-----------|
| Secunia (*) | 15.36% | 15.36% |
| SecurityFocus (*) | 13.08% | 28.44% |
| IBM ISS X-Force (*) | 12.36% | 40.80% |
| BugTraq | 11.23% | 52.03% |
| Miscellaneous | 6.50% | 58.53% |
| FrSIRT (*) | 6.47% | 65.00% |
| OSVDB | 5.29% | 70.29% |
| SecurityTracker (*) | 4.05% | 74.34% |
| Sreason | 2.46% | 76.80% |
| CERT (*) | 2.28% | 79.08% |



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.



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



Measurements



Advisories by Source

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

- 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

| Source | % ISS | SF | Secunia | FrSIRT |
|---------|--------------|--------------|--------------|--------------|
| ISS | 6,022 92% | 6,264 95% | 6,437 99% | 6,416 98% |
| SF | | 4,797 73% | 5,802 89% | 5,637 86% |
| Secunia | | | 4,535 69% | 5,042 77% |
| FrSirt | | | | 3,842 59% |

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

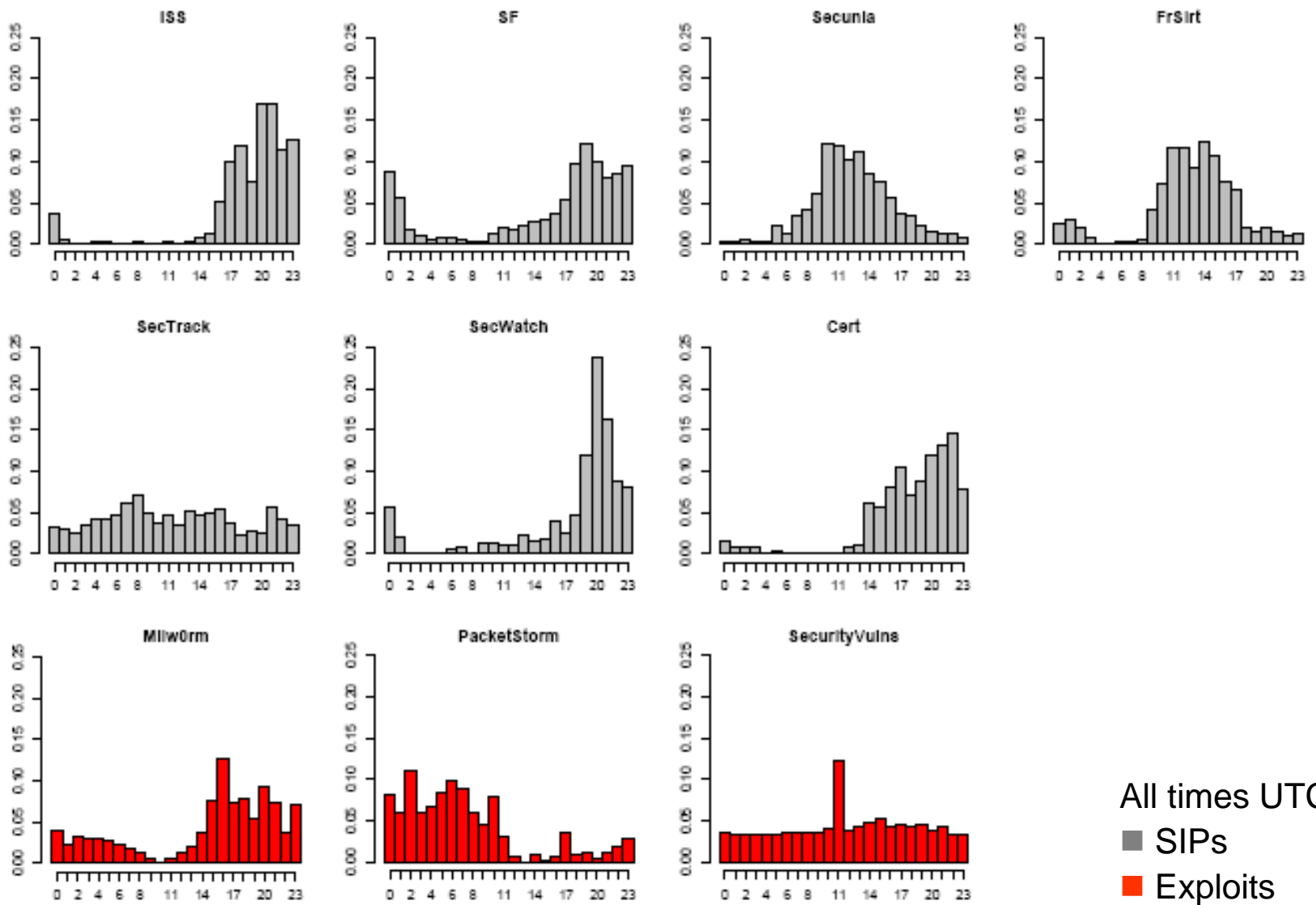


Publication Dynamics

- 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.



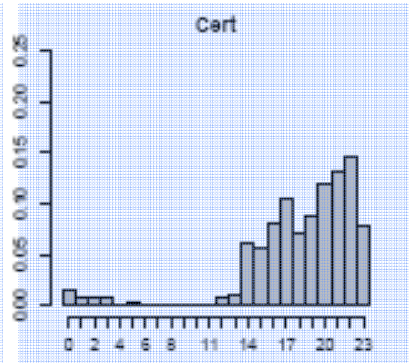
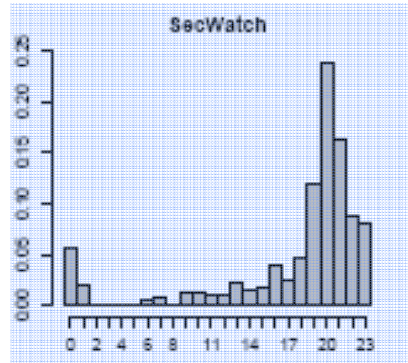
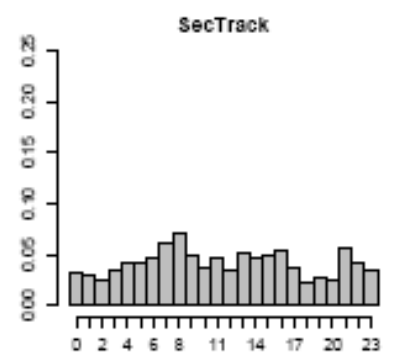
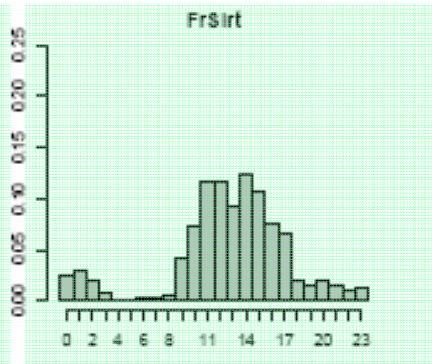
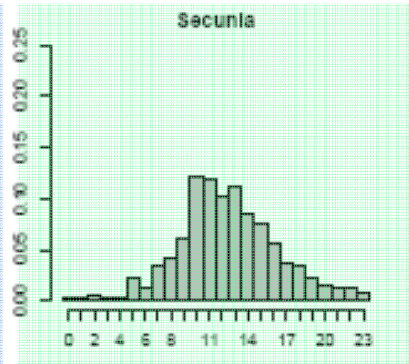
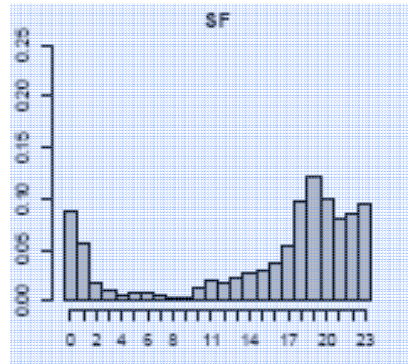
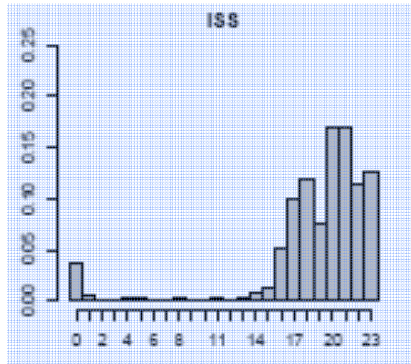
By the hour of the day



All times UTC
■ SIPs
■ Exploits

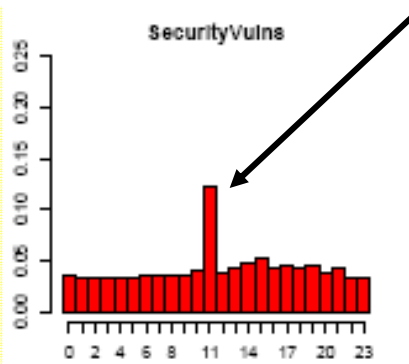
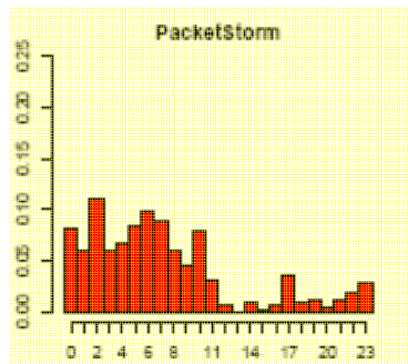
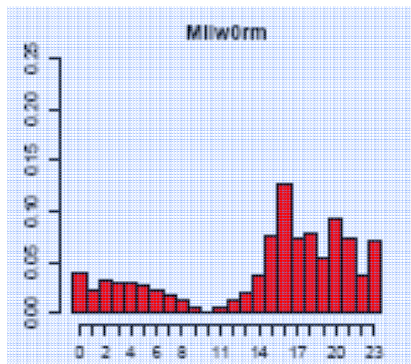


By the hour of the day



Time zones

- Americas
- Europe
- Far East



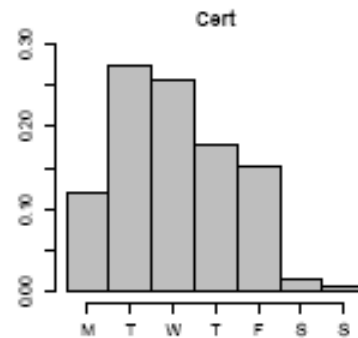
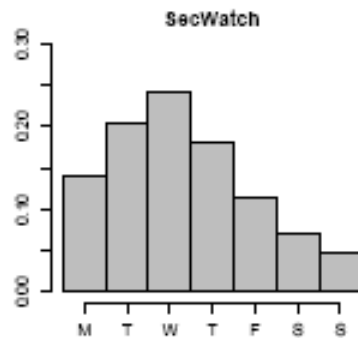
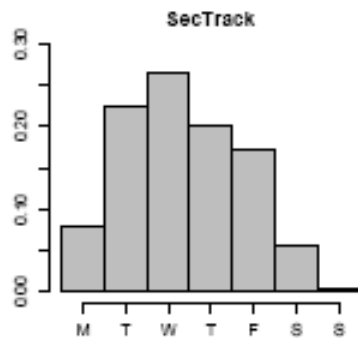
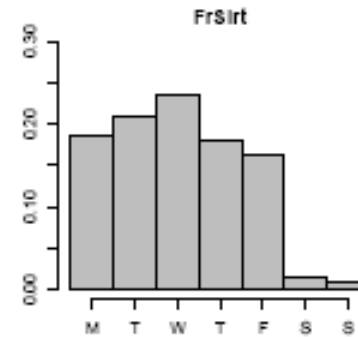
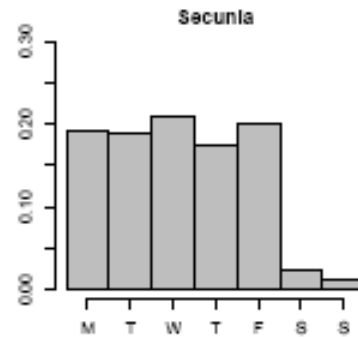
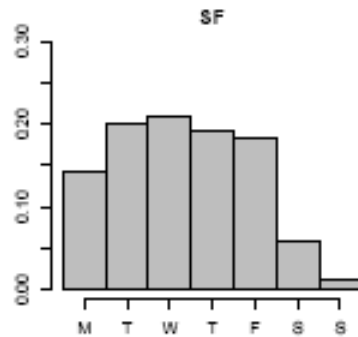
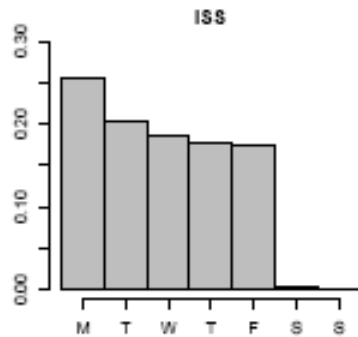
Automated Tools?

All times UTC

- SIPs
- Exploits

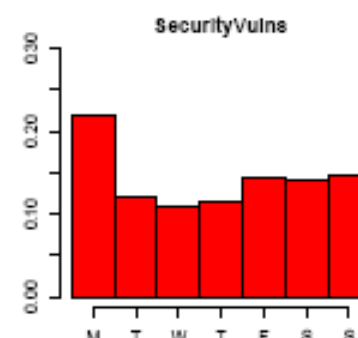
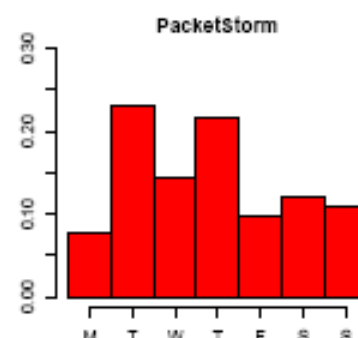
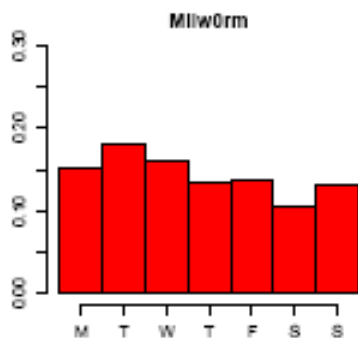


By the day of the week



SIPS (the good):
low weekend activity

Exploits (the bad):
uniform activity throughout the week



All times UTC
 ■ SIPS
 ■ Exploits



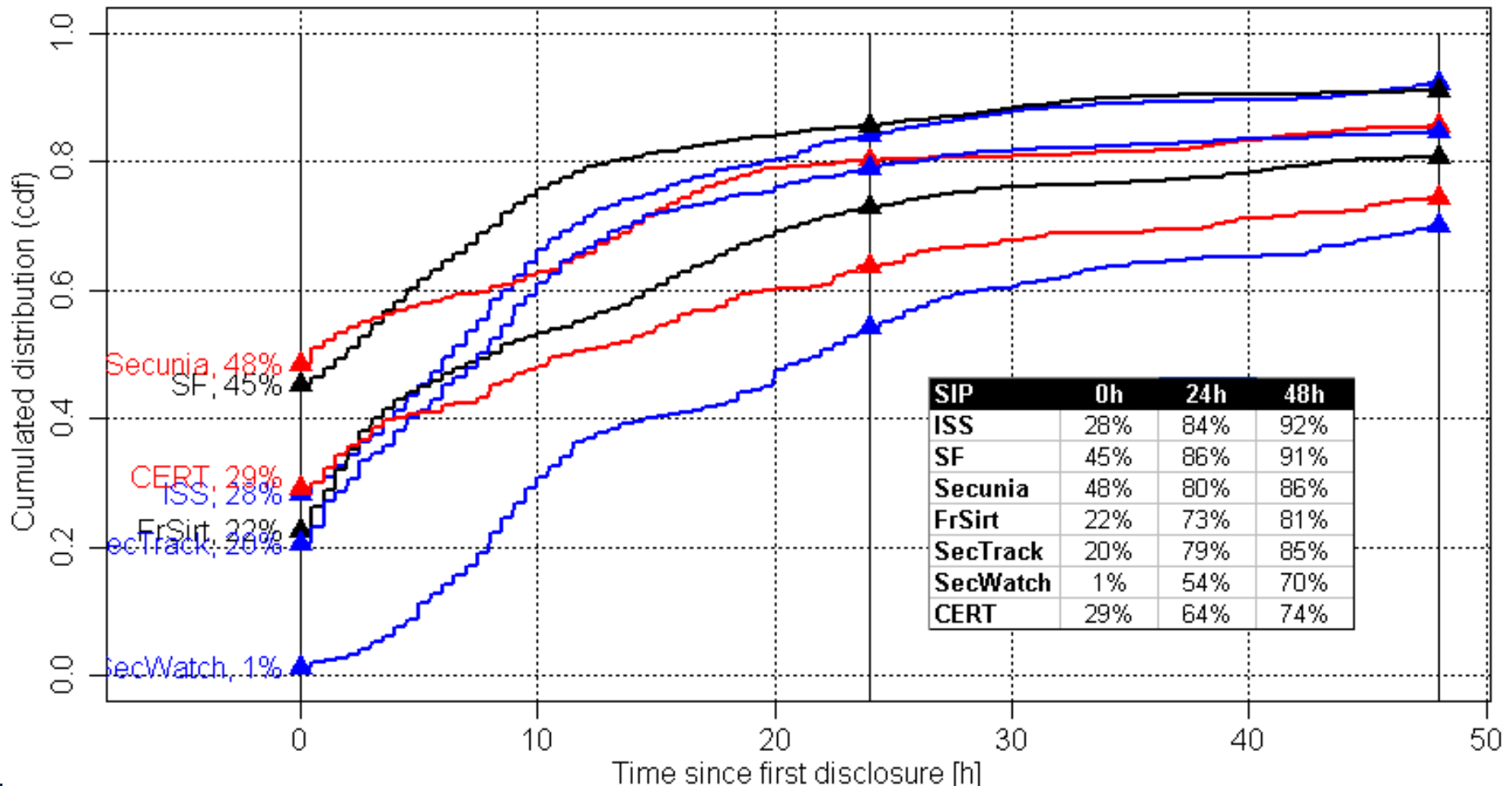
Performance Comparison

- 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.

Disclosure delay (0-48 h)





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.



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich



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



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Swiss Federal Institute of Technology, Zurich

www.csg.ethz.ch