

The Dynamics of (In)Security

What's the story of 30,000 vulnerabilities discovered in the past decade?

3rd Athens International Forum on IT Security - 2010

Dr. Stefan Frei, ETH Zürich





Abstract

We examine the security ecosystem, consolidating many aspects of security that have hitherto been discussed only separately. Based on a quantitative analysis of 30,000 vulnerabilities disclosed over the past decade we quantify the systematic gap between exploit and patch availability. This analysis provides a metric for the success of the "responsible disclosure" process, the prevalence of the commercial markets for vulnerability information and highlight the role of security information providers (SIP), which function as the "free press" of the ecosystem.

Vulnerability Lifecycle and Ecosystem

There is no security on this earth, only opportunity
Douglas MacArthur (1880-1964)





Vulnerabilities

- What is a vulnerability?
 - “it’s a feature, not a vulnerability”, says vendor
- Security vulnerability
 - “refers to a weakness in a system allowing an attacker to violate the confidentiality, integrity, availability of the system or the data and applications it hosts.”
 - many similar definitions exist
 - the security landscape is defined by vulnerabilities



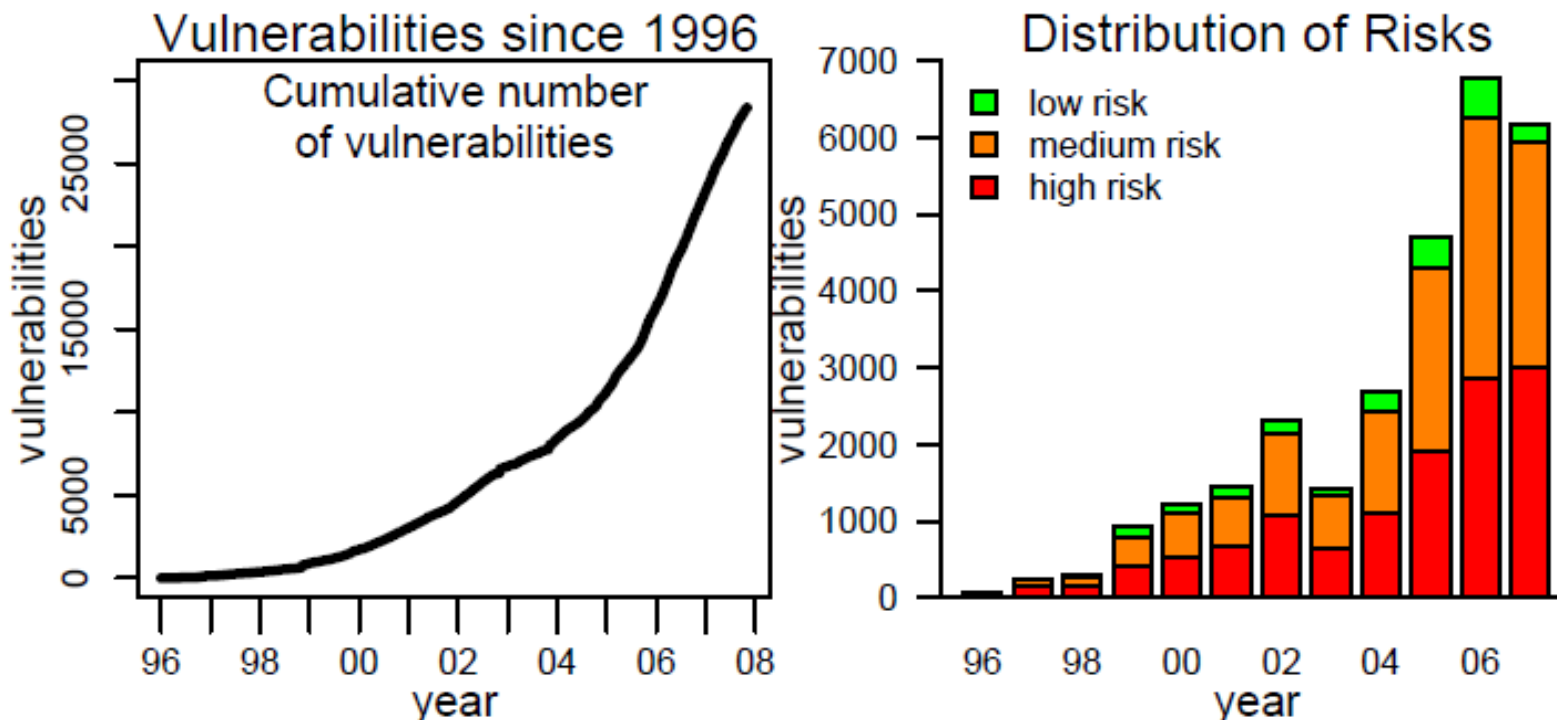
CVE - standardized vulnerability names

- Common Vulnerability Exposures (CVE)
 - CVE aims to standardize the names for all publicly known vulnerabilities and security exposures
 - CVE has become a de facto industry standard of vulnerability identifiers
 - Sample: CVE-2010-0249
- Any security issue of relevance will eventually get a CVE number assigned
- Source
 - <http://cve.mitre.org>
 - <http://nvd.nist.gov>



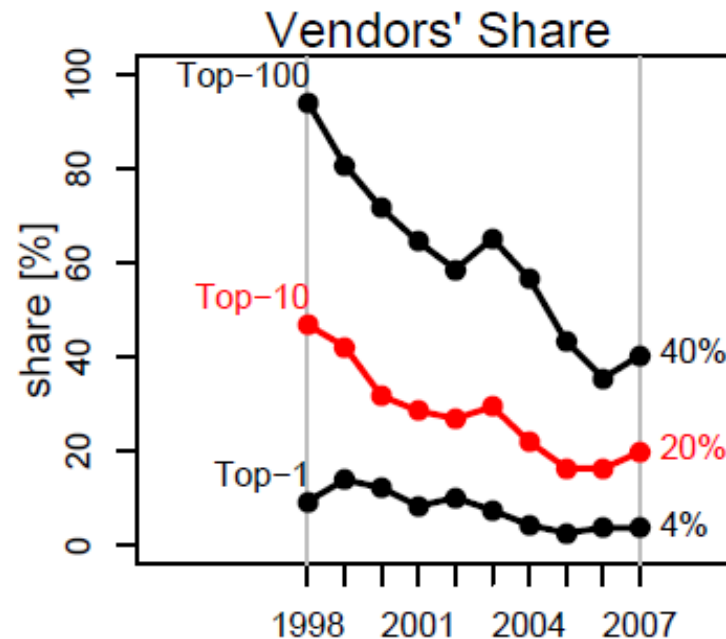
Vulnerability counts

- 40'000+ disclosures (CVEs) since 1996 ..



Vendor - vulnerabilities distribution

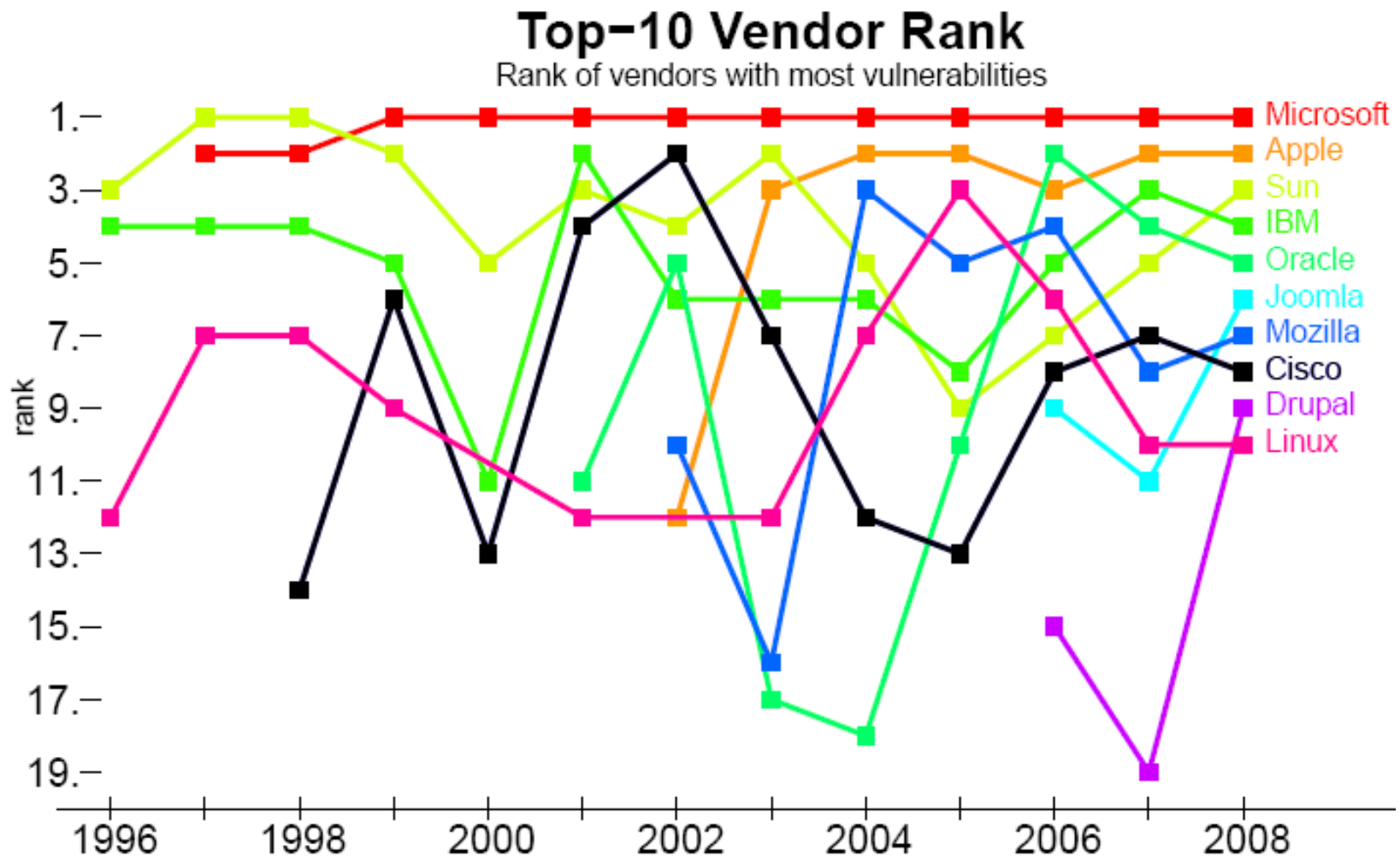
- Few vendors account for most vulnerabilities
- Rank of vendors' vulnerabilities 2000-2007
- The top-10 vendors account for 20% of all vulnerabilities



2000:	1,217 vulns	433 vendors	681 products
2008:	5,996 vulns	2,427 vendors	4,212 products

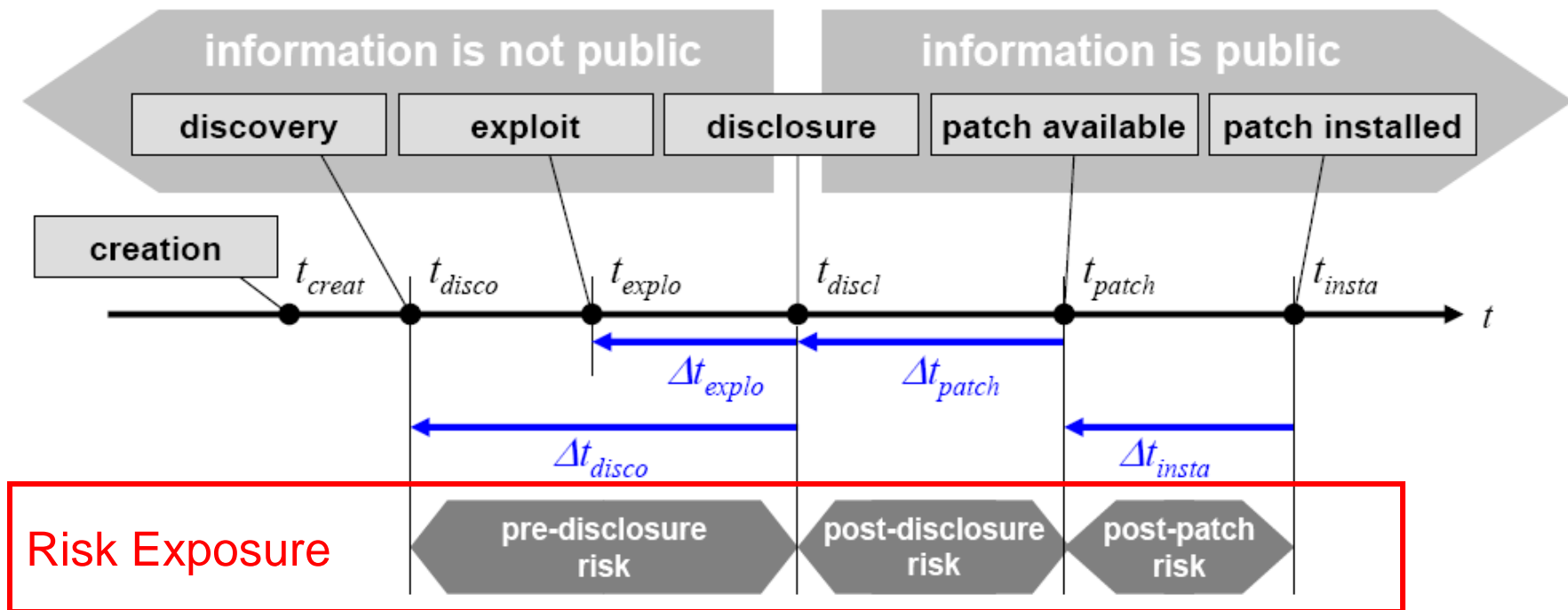


Vendors with most vulnerabilities



Lifecycle of a vulnerability

- from vulnerability discovery to patch
- the sequence and timing of events determines risk exposure





Risk Exposure

- Pre-disclosure risk (exogenous)
 - time from **discovery** to **disclosure**
 - only a closed group is aware of the vulnerability
 - this group could be anyone from hackers, organized crime or responsible security researchers/vendors

- Post-disclosure (exogenous)
 - time from **disclosure** to **patch**
 - user waits for the vendor to issue a patch
 - public is aware of this risk but has not yet received remediation from vendor

- Post-patch risk (endogenous)
 - the time from **patch availability** to **patch installation**



Vulnerability Disclosure

- our requirements for the disclosure date:
 - vulnerability information is freely available to the public
 - disclosed by a trusted and independent source
 - vulnerability is analyzed and risk-rated by experts

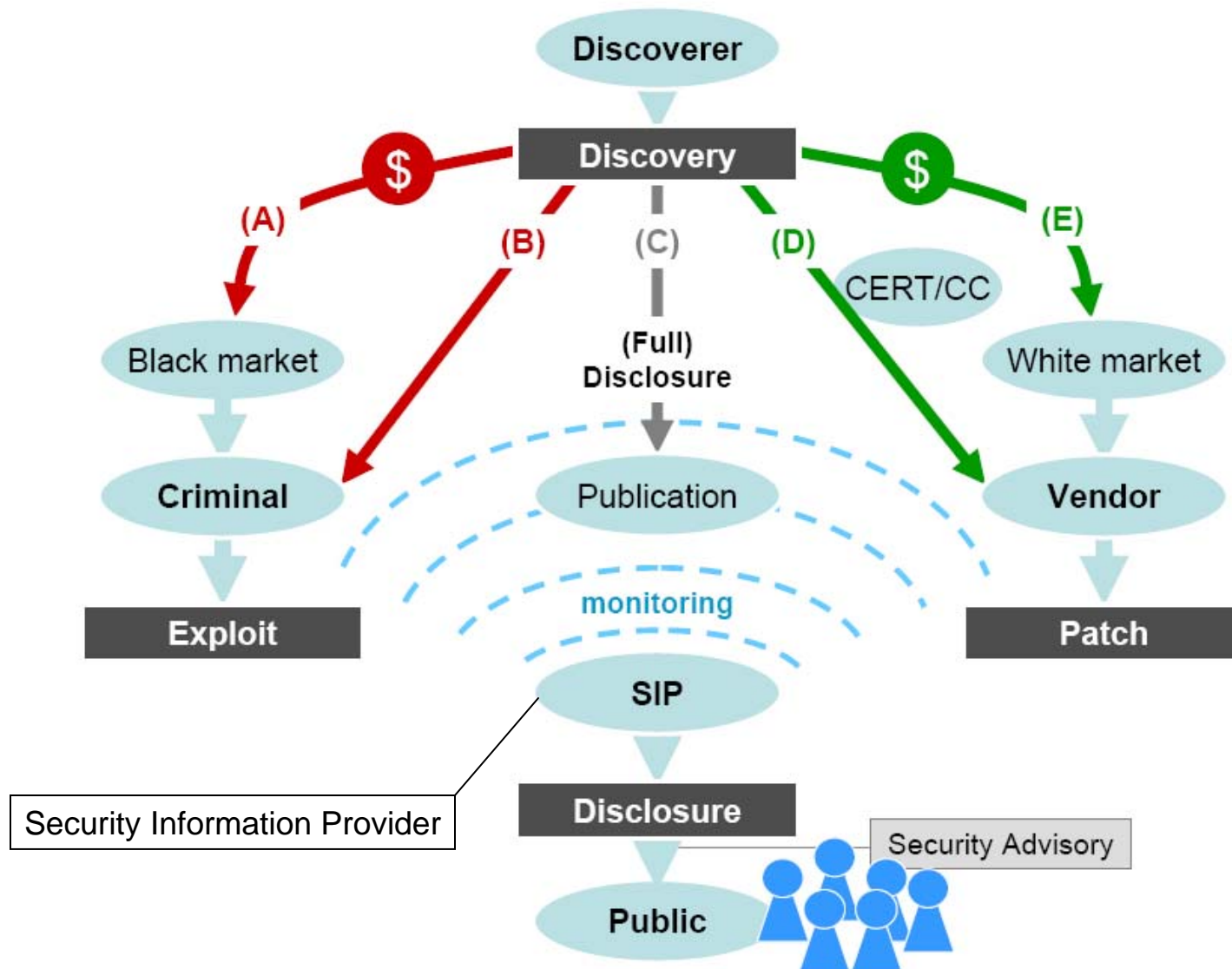
- who can provide this information?
 - Security Information Providers (SIP)
 - what is the performance of these services?



Vulnerability discovery

- how vulnerability information is handled is exclusively the discoverers choice:
 - economics, discoverer ethics, and past experience determine the process following the discovery
 - some processes benefit the security, others the insecurity
 - in any case the end-user of the software is exposed to vulnerabilities and has no direct control over the game

The Security Ecosystem



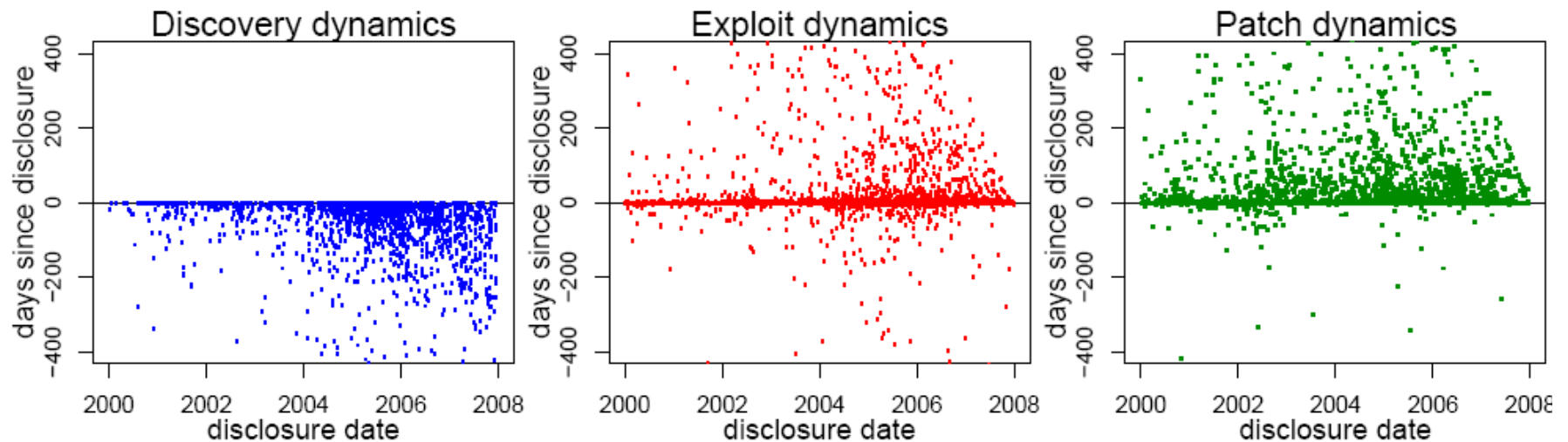


Role of Security Information Provider SIPs

- **Independent and trusted SIPs act like the free press in an open society: they are efficient watchdogs to expose important issues to the public!**
 - issues addressed by a SIP are hard to be denied by either the vendor or a government
 - this is an essential role for the well-being and functioning of the security ecosystem

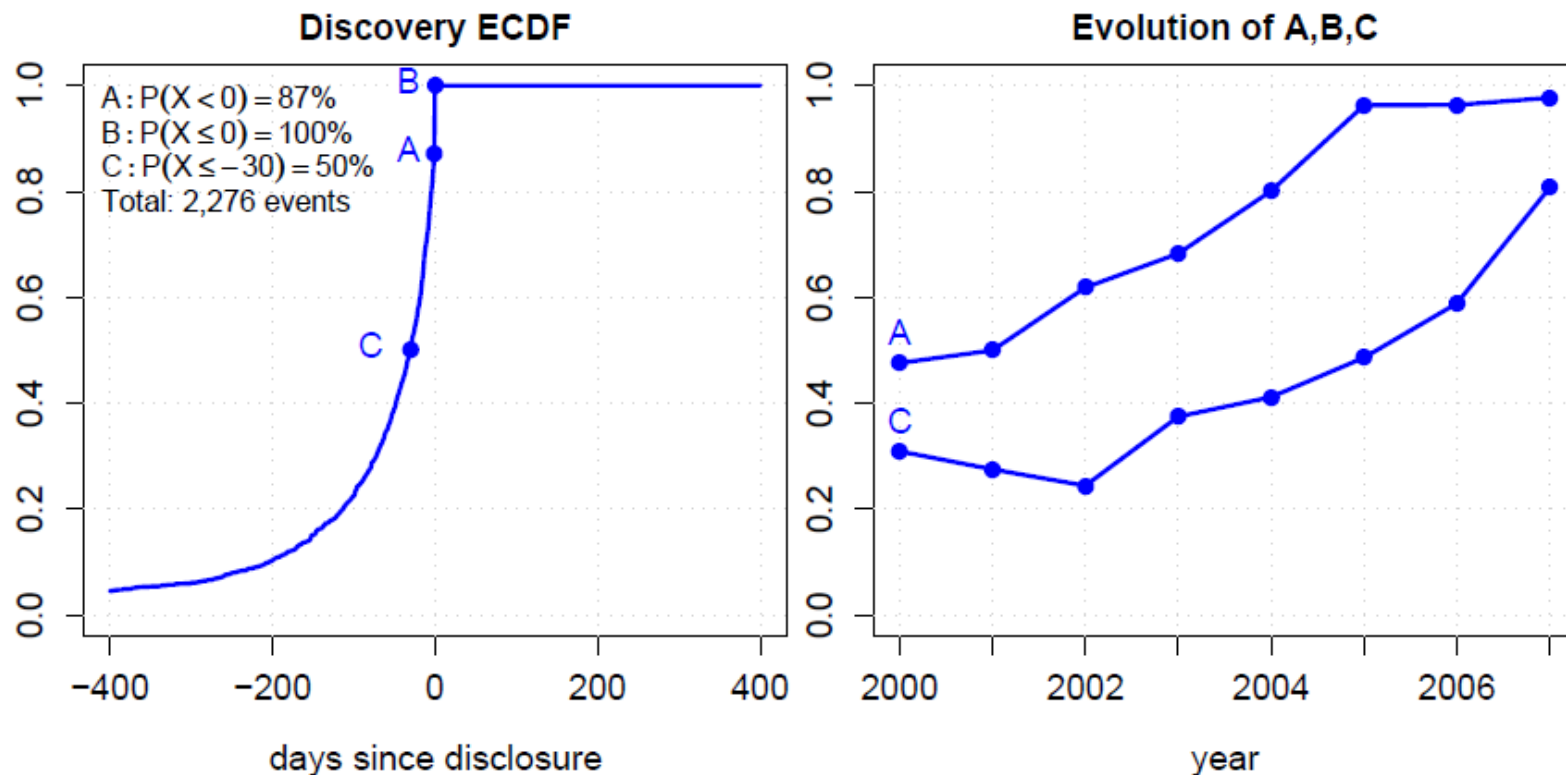
Measurement data

- the dynamics of lifecycle events
 - analysis of more than 27,000 vulnerabilities (CVEs) 1996-2007
 - 2,276 discovery dates
 - 9,243 exploit availability dates
 - 3,593 patch availability dates
- normalized to disclosure date of vulnerability



Discovery dynamics

- measure of pre-disclosure risk
- 50% of vulns known to insiders 30 or more days before disclosure (less-than-zero-day)





From discovery to disclosure

- less than zero day
 - vulnerabilities not yet known to the public are systematically used by:
 - Hackers
 - Spammers and Phishers
 - Governments, Military (Bundestrojaner)

- there is a market for new vulnerabilities
 - ZeroDayInitiative of Tipping Point, iDefense
 - black market
 - prices from 1,000 to 75,000 USD offered

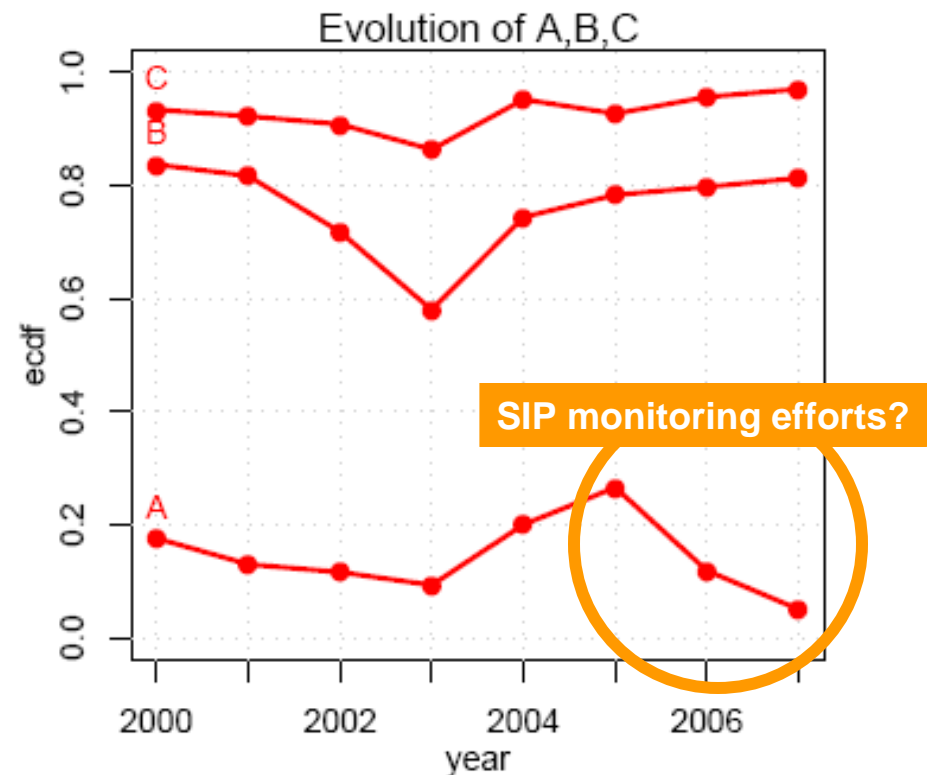
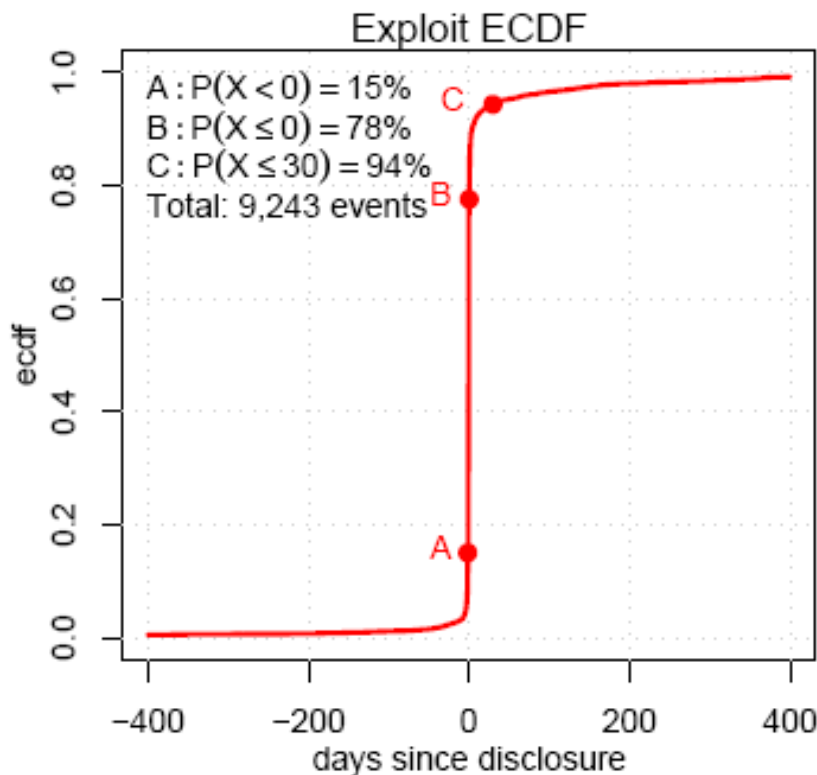
Pending vulnerabilities as of 28-Sep-07

ZDI ID	Affected Vendor	Severity	Reported On
ZDI-CAN-047	IBM	High	2006.06.16, 469 days ago
ZDI-CAN-063	Computer Associates	High	2006.09.12, 381 days ago
ZDI-CAN-088	Computer Associates	High	2006.09.12, 381 days ago
ZDI-CAN-103	Microsoft	High	2006.09.14, 379 days ago
ZDI-CAN-105	Hewlett-Packard	High	2006.10.10, 353 days ago
ZDI-CAN-111	Hewlett-Packard	High	2006.10.10, 353 days ago
ZDI-CAN-125	IBM	High	2006.11.09, 323 days ago
ZDI-CAN-134	Hewlett-Packard	Medium	2006.12.18, 284 days ago
ZDI-CAN-137	Novell	High	2007.01.08, 263 days ago
ZDI-CAN-143	Computer Associates	High	2007.01.12, 259 days ago
ZDI-CAN-141	RealNetworks	High	2007.01.17, 254 days ago
ZDI-CAN-159	Oracle	High	2007.01.29, 242 days ago
ZDI-CAN-160	Oracle	High	2007.01.29, 242 days ago

Source: http://www.zerodayinitiative.com/upcoming_advisories.html

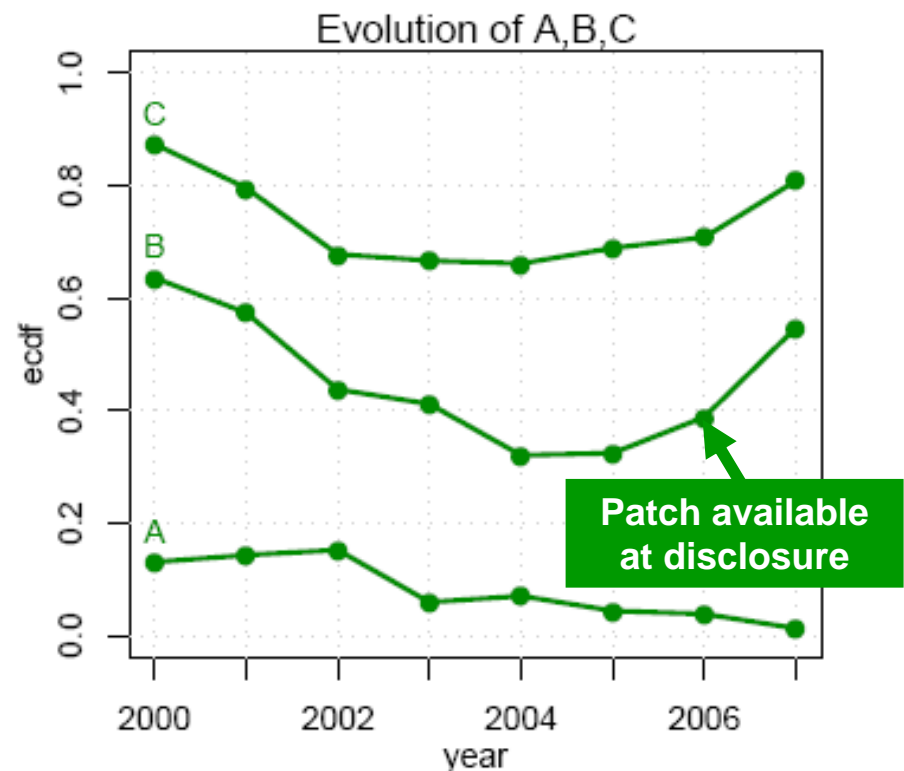
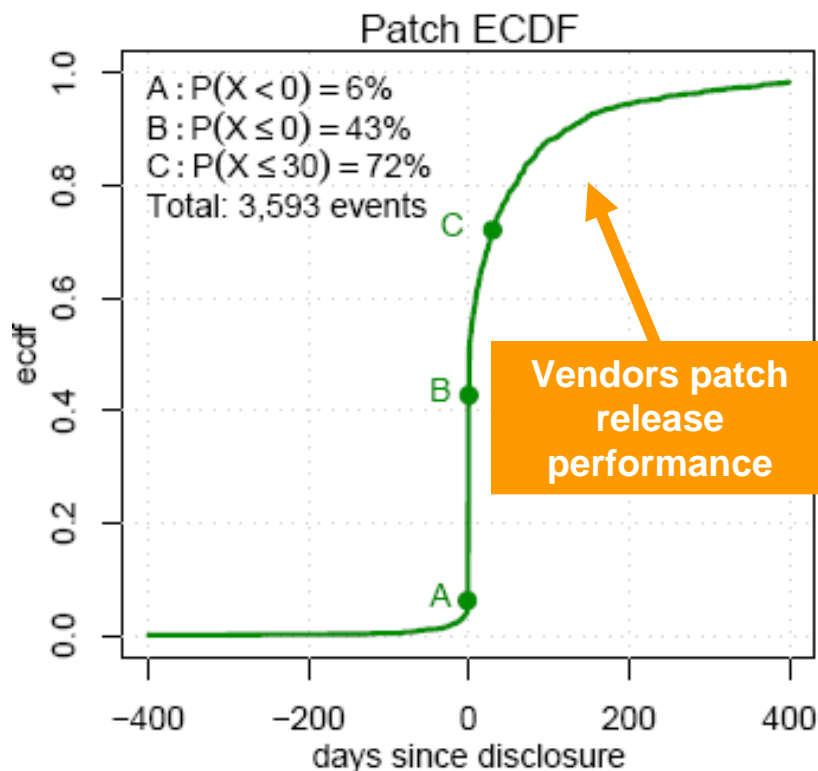
Exploit dynamics

- rise of exploit availability from 15% to 78% at disclosure
- minimum estimator for # of exploits available to cyber-criminals



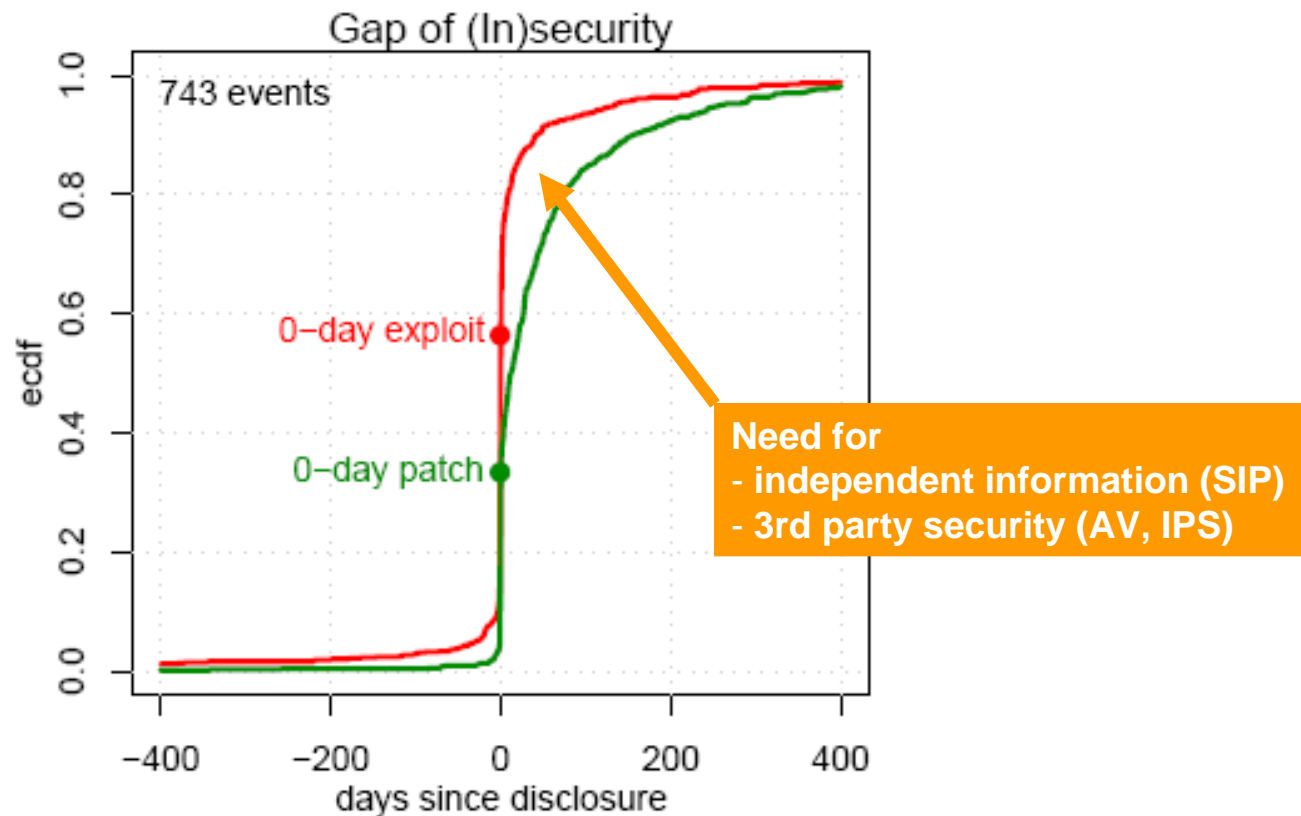
Patch dynamics

- 43% zero-day patch availability (B)
 - a measure of responsible disclosure process
- measures vendors' patch release performance, an estimator of „post-disclosure“ risk



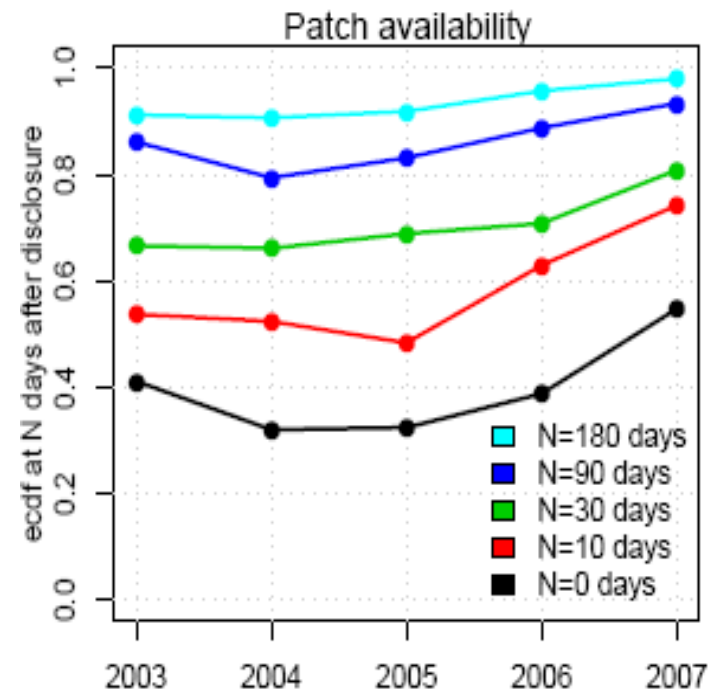
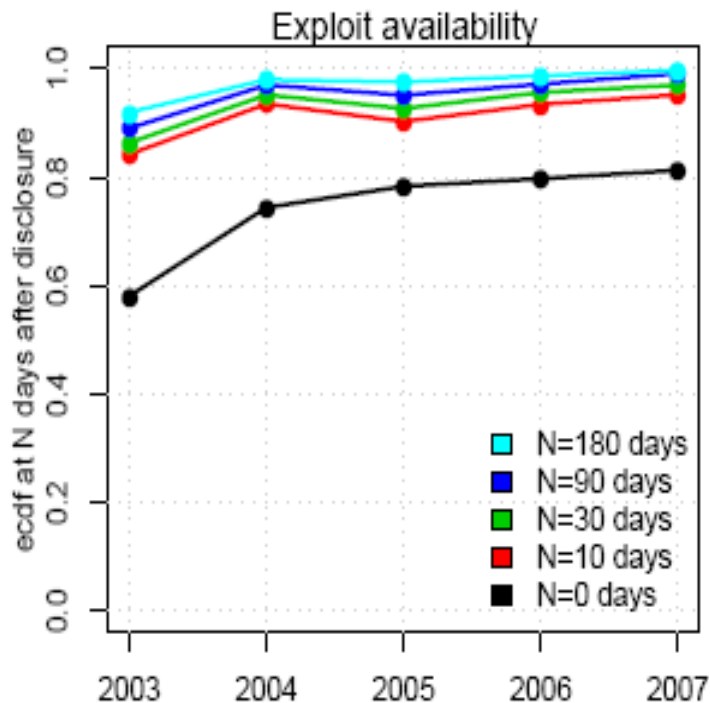
The gap of (In)security

- exploit availability exceeds patch availability
- exploit and patch development follow fundamentally different processes - favoring the bad



The gap of (In)security 2003 - 2007

- exploit availability consistently exceeds patch availability
- patch availability seems to increase since 2005
- many unpatched vulnerabilities 180 days after disclosure





Concluding remarks

- The Security Ecosystem model relates events of the **vulnerability lifecycle** to **processes** in the security ecosystem
- Independent Security Information Providers (SIP) are key (comparable to the role of the **free press**)
- Methodology based entirely on **publicly available data**
- Systematic **gap in exploit vs. patch availability**



Thank you

- Contact: Dr. Stefan Frei
- <http://www.techzoom.net>



Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Summary, References, Glossary





Security Information Providers (SIP)

- **Secunia** (Secunia, Denmark)
www.secunia.com, since 2002
- **IBM X-Force** (IBM Internet Security Systems, USA)
www.iss.net, since 1996
- **Securityfocus** (Symantec, USA)
www.securityfocus.com, since 1996
- **CERT** (Computer Emergency Response Team, USA)
www.cert.org, started before 1996
- **FrSirt** (French Security Incident Response Team, France)
www.frsirt.com, since 2004