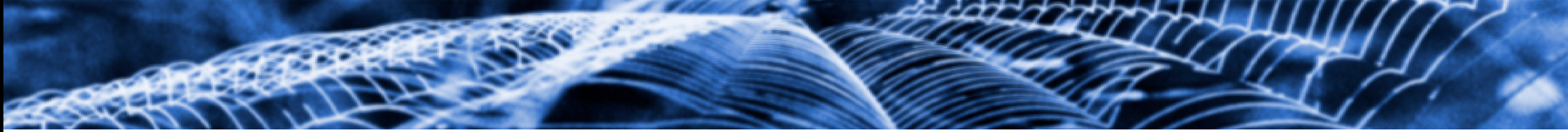


The speed of (in)security

Analysis of the speed of security vs insecurity

BlackHat 2006 USA – Las Vegas

Stefan Frei + Martin May
Communication Systems Group
ETH Zurich – Switzerland
http://www.csg.ethz.ch
http://www.techzoom.net/risk

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Abstract

To understand the security risks inherent with the use and operation of today's information and communication systems, analysis of the vulnerabilities' technical details is not sufficient. Defending against attacks requires a quantitative understanding of the vulnerability lifecycle (e.g. *the discovery-, disclosure-*, *exploit-* and *patch-date*).

Specifically, one has to understand how exploitation and remediation of vulnerabilities, as well as the distribution of information thereof is handled by the industry.

While the explanation of the discovery-, exploit-, and patch-date is rather intuitive, we propose a new defnition for the disclosure-date of a vulnerability.

In our research, we examine how vulnerabilities are handled in large-scale, analyzing more than 80,000 security advisories published since 1996. Based on this information, we quantify and discuss the gap between the time of exploit- and patch-availability: the dynamics of (in)security.

Motivation

Large scale risk assessment

- for risk assessment, the knowledge of technical details of vulnerabilities is not sufficient
- timing is essential (patch- vs exploit-availability)
- vulnerability disclosure-date not yet suitably defined

Contributions

- we propose a concise definition for the disclosure-date
- we present an analysis of 14,000+ vulnerabilities 1996..
- we propose a methodology to measure security risk

Outline

- Revisiting the vulnerability **disclosure-date**
- Comparing **Security Information Providers** (SIP)
- Analysis of the relation between discovery-, exploit-, and patch-dates
- Distribution functions and trends
- Conclusion

What is the disclosure-date?

- first discussion of a potential vulnerability in a security list?
- vage information from vendor (e.g. with patch)?
- rumors?

.. these do not qualify as disclosure-date!

Our requirements:

- vulnerability information is freely available to public
- disclosed by a trusted and independent source
- vulnerability is analyzed and rated by experts

Definition of the disclosure-date

To ensure the quality and availability of relevant security information, we propose the following definition of the disclosure-date:

The time of disclosure is the first date a vulnerability is described on a channel where the disclosed information on the vulnerability fullfills the following requirements:

The vulnerability information ..

1. is freely available to the public.
2. is published by trusted and independent channel.
3. was analyzed by experts that risk rating information is included in the disclosure.

Requirement details

Requirement 1

From the security perspective, only a free and public disclosure can ensure that all interested parties get the relevant information. Security through obscurity is a concept that never worked.

Requirement 2

Only a channel independent of a vendor or a government is unbiased and enables a fair dissemination of security critical information. A channel is considered trusted when it is a widely accepted source of security information in the industry (e.g by having reliably delivered security information over a long period of time).

Requirement 3

Analysis and risk rating ensures the quality of the disclosed information. The mere discussion on a potential flaw in a mailing list or vage information from a vendor do therefore not qualify.

Security Information Providers

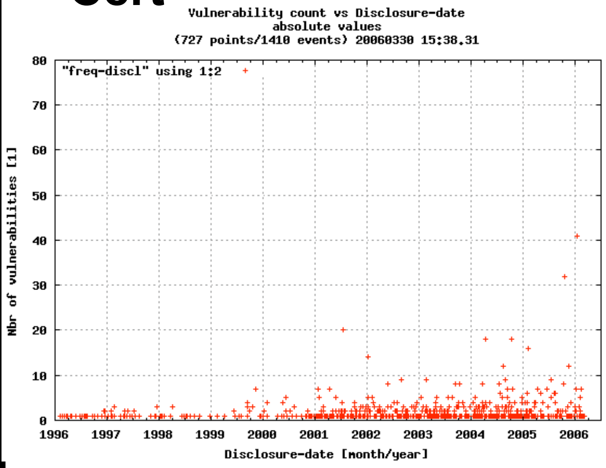
Potential providers for the disclosure-date

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

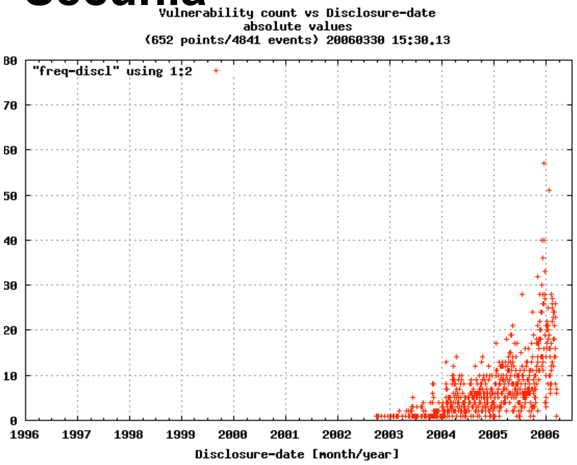
Candidates to provide the disclosure-date

Number of vulnerabilities disclosed per day from 1996-2006

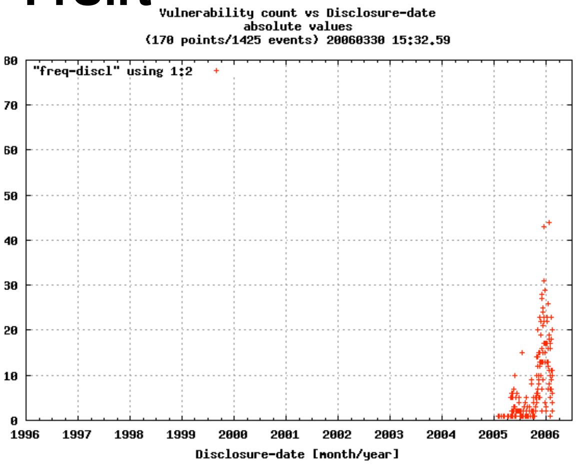
Cert



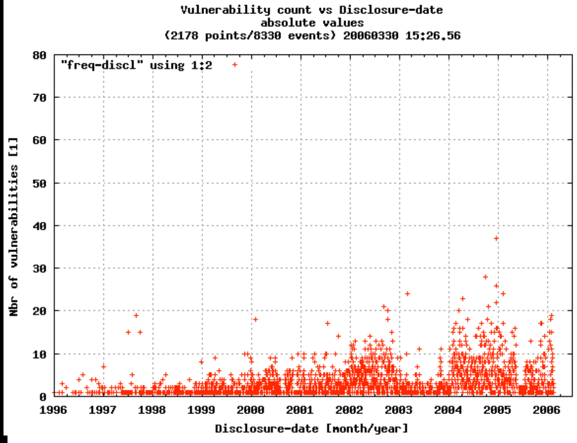
Secunia



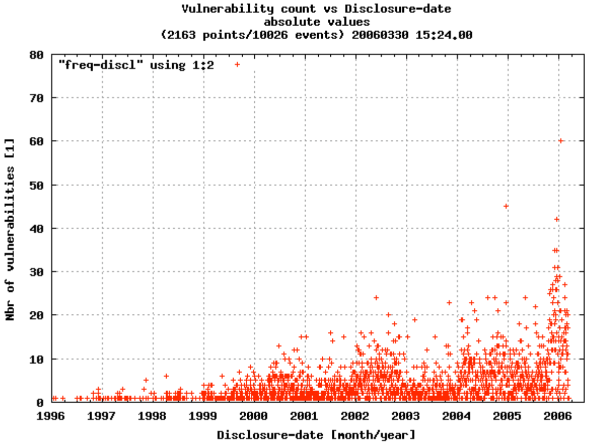
FrSirt



ISS x-Force



Securityfocus



ISS+Securityfocus:

- well established
- long history
- largest dataset

Secunia+FrSirt good for recent vulnerabilities

Data and analysis

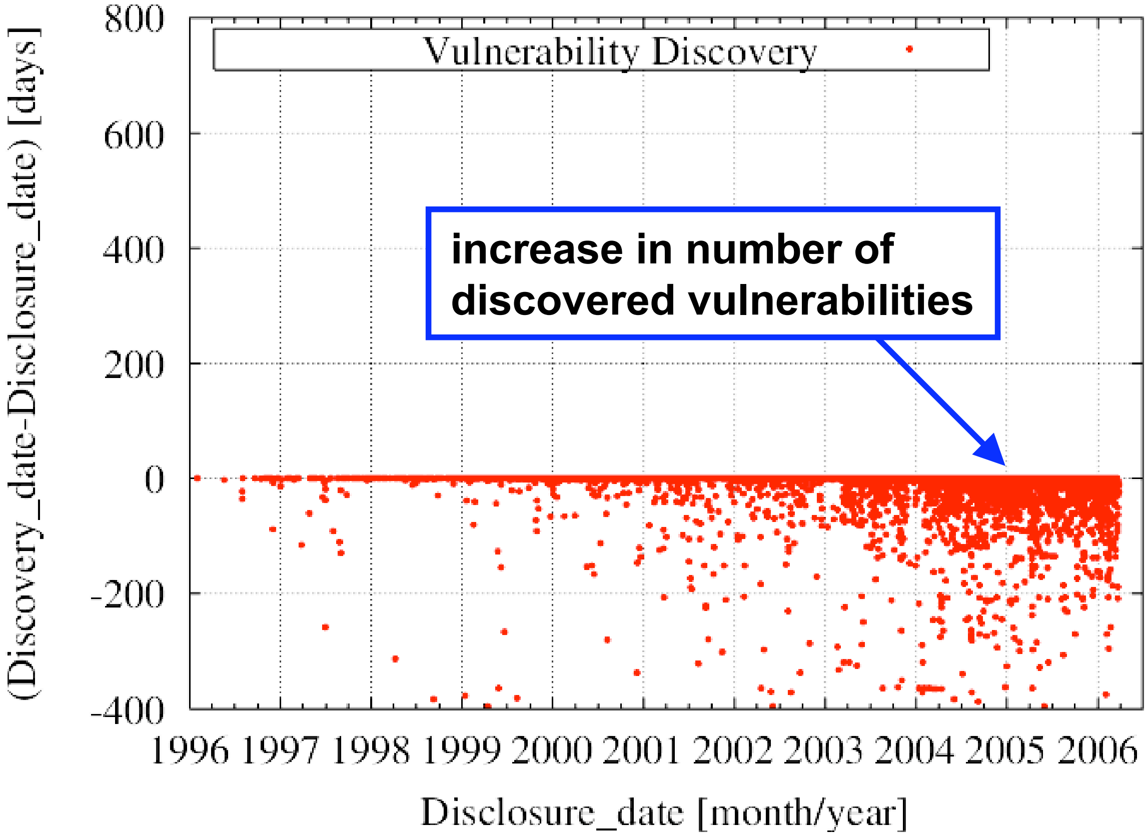
Data used for this analysis

- Disclosure-date
  - taken from **ISS X-Force** or **Securityfocus**, whichever is earlier
  - well known sources, data available since 1996, they differ only slightly
  - two data providers. potential bias for own products neutralized
- Vulnerabilities from NVD[1] and OSVDB[2]
  - 14,000+ vulnerabilites with a CVE entry and risk metric information
  - correlated with information from 80,000+ security advisories
- Relation between **disclosure-date** and
  - **discovery-date** available for some vulnerabilities, usually after disclosure
  - **exploit-date** from known exploit sites (milw0rm, frsirt, metasploit, ..)
  - **patch-date** from vendor, originator of the software

[1] www.nvd.nist.gov, [2] www.osvdb.org

Discovery-date Analysis

Discovery-date vs disclosure-date



increase in number of discovered vulnerabilities

Y-Axis:

days between **discovery- and disclosure-date** **in days**

X-Axis:

disclosure-date

Data

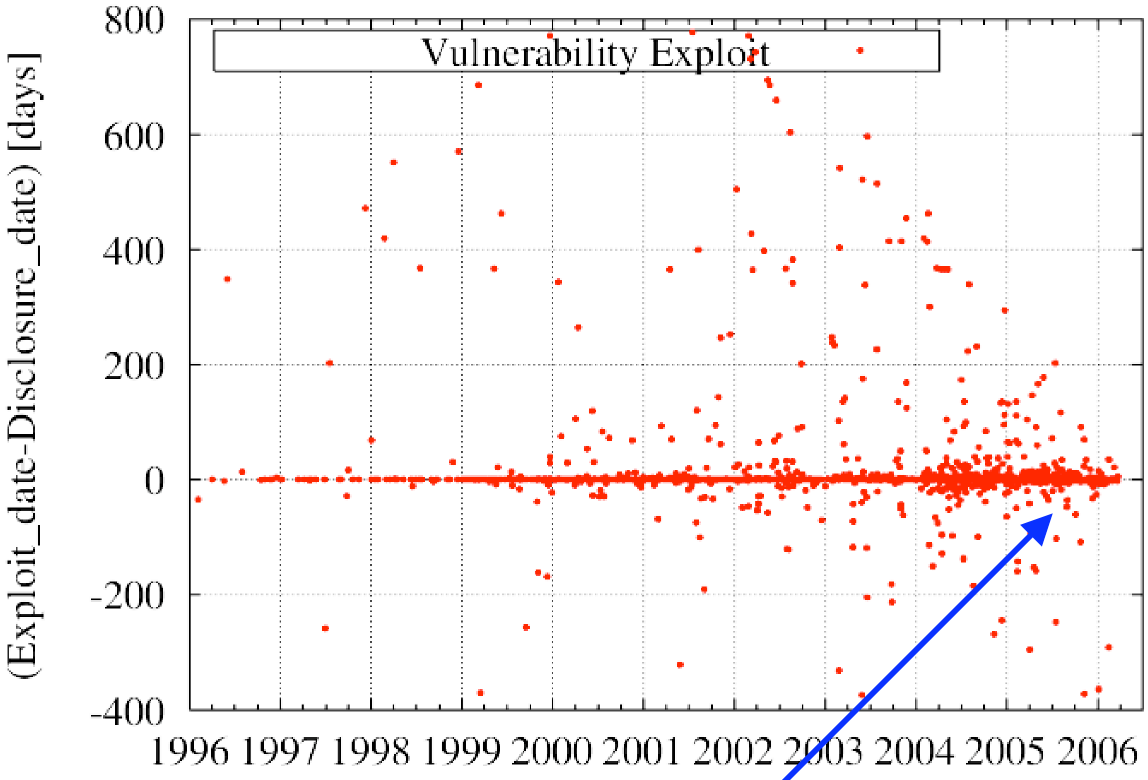
- 9733 discovery dates

- 42% before disclosure

- 58% at disclosure

Exploit Availability

Exploit availability date vs disclosure-date



higher concentration near disclosure-date: 0-day exploits

Y-Axis:
days between exploit- and disclosure-date in days

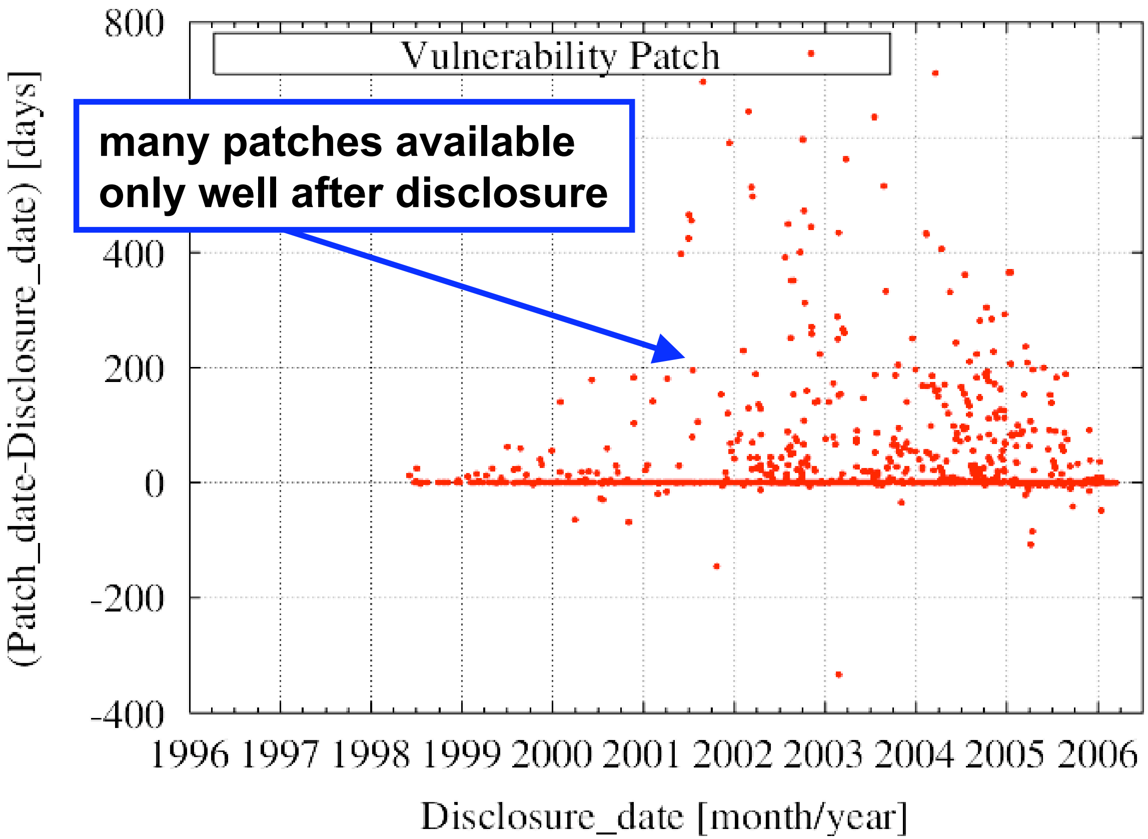
X-Axis:
disclosure-date

Data
- 3428 exploits

- 23% before disclosure
- 58% at disclosure
- 19 % after disclosure

Patch Availability

Patch availability date vs disclosure-date



many patches available only well after disclosure

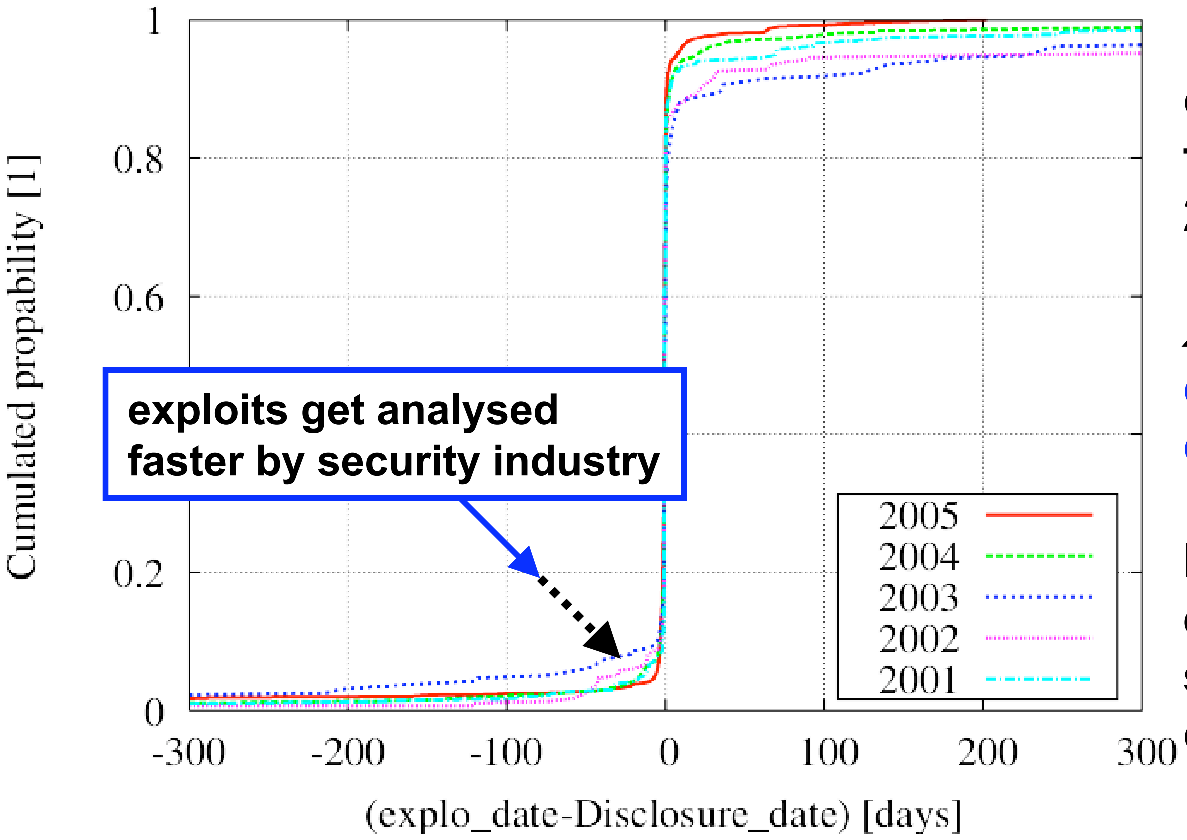
Y-Axis:
days between patch- and disclosure-date in days

X-Axis:
disclosure-date

Data
-1551 patches

- 15% before disclosure
- 54% at disclosure
- 31% after disclosure

Exploits per year



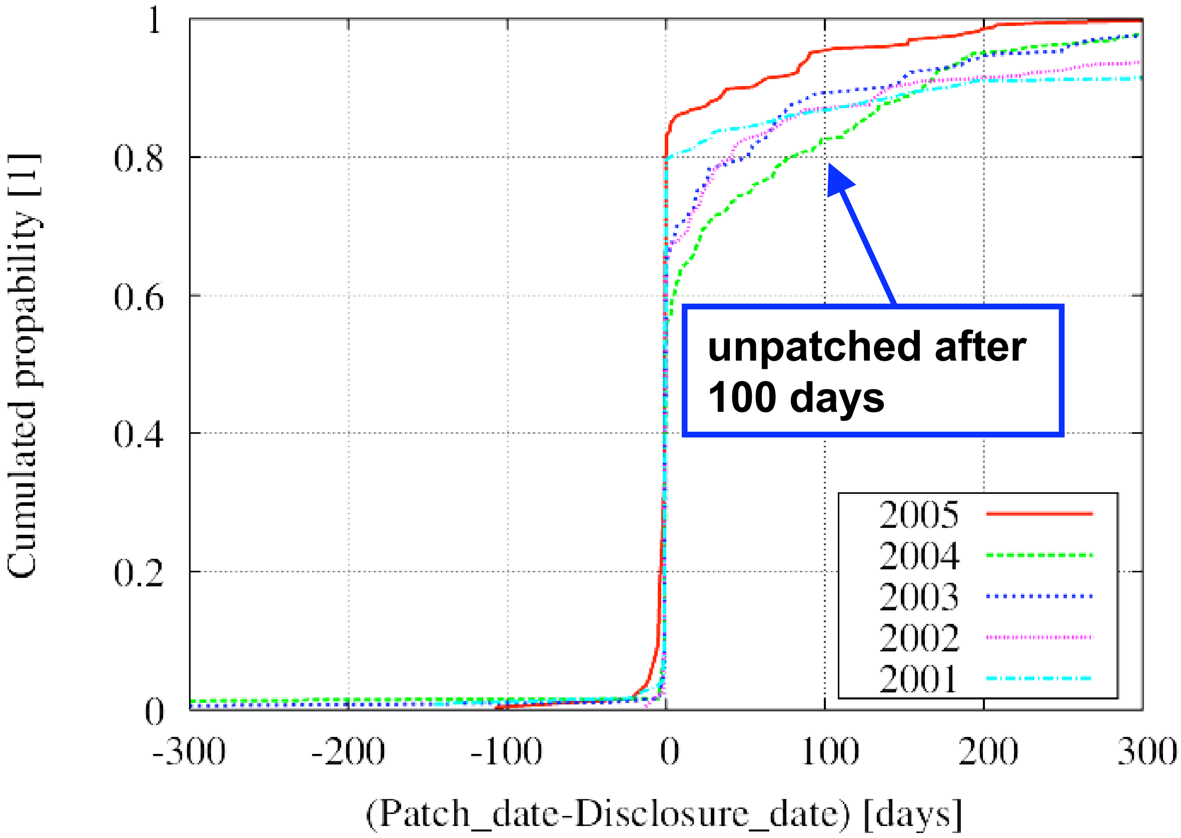
exploits get analysed faster by security industry

Y-Axis:
cumulated probability for **exploit dates** **2001-2005**

X-Axis:
days from disclosure-date

Increasing number of exploits available at (or short after) the disclosure-date

Patches per year



Y-Axis:

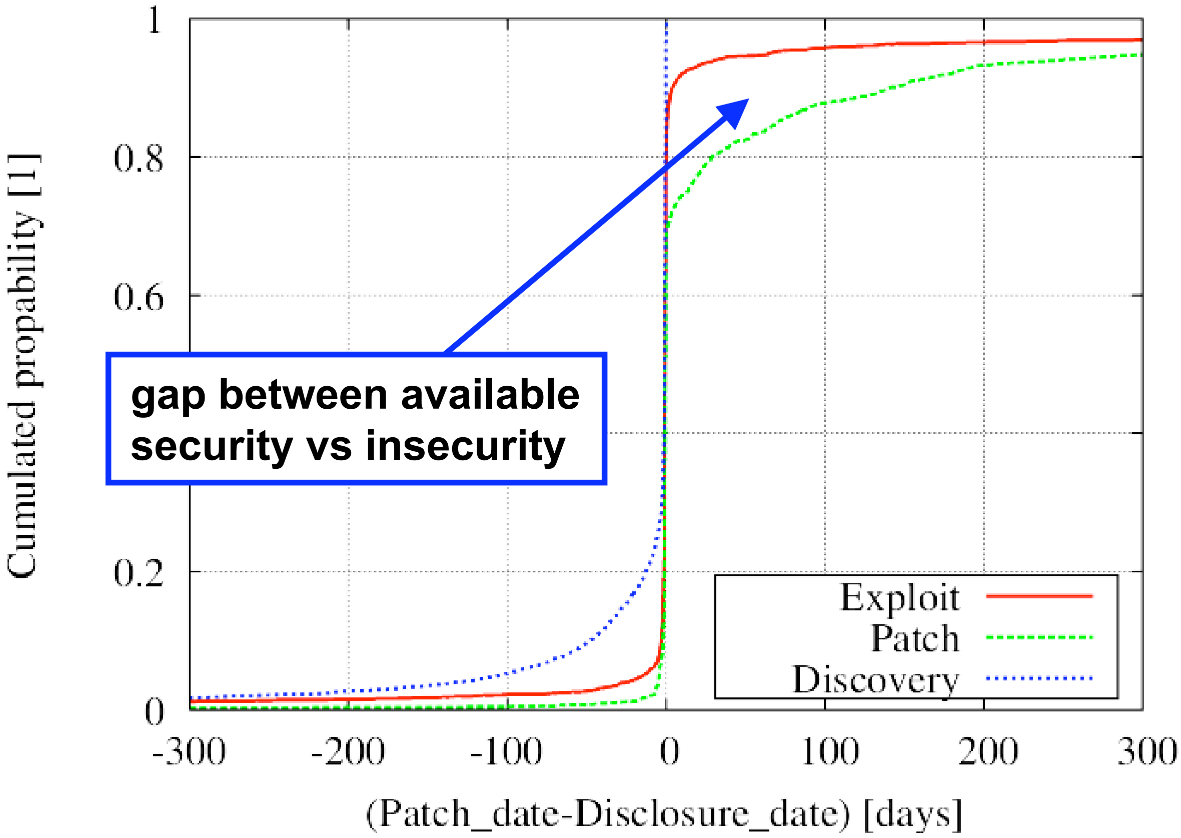
cumulated probability for patch-dates 2001-2005

X-Axis:

days from disclosure-date

The Speed of (In)security

The dynamics of security vs insecurity



gap between available security vs insecurity

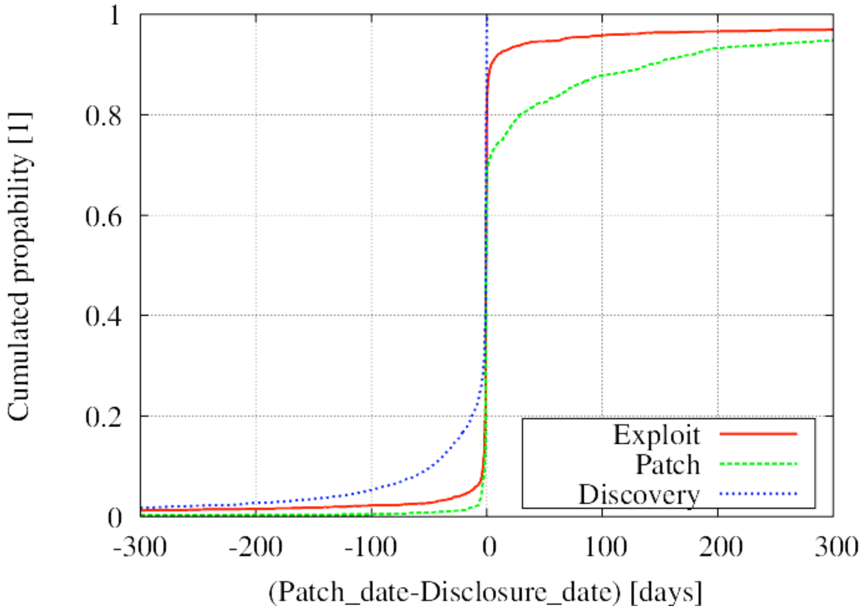
Y-Axis:
cumulated probability for exploit- and patch-availability dates

X-Axis:
days from disclosure-date

Data:
- **3416 exploits**
- **1477 patches**
- **from 1996-2006**

Interpretation – Risk Metric

We see that the exploit-CDF remains above the patch-CDF over the full range of 300 days after disclosure. This gap, which quantifies the difference between exploit- and patch-availability, indicats the risk exposure and its development over time. This metric enables us to empirically measure and assess the state of the security industry.



CDF
Cummulated Distribution Function

Conclusion

- first analysis of relation between patch- and exploit-dates on this scale
- large dataset (14,000+ vulnerabilites, 80,000+ advisories)
- measured gap between patch- and exploit-availability

Future

- continued monitoring and database updates
- online risk analysis tool at `www.techzoom.net/risk`

Thank you

Thank you

- All plots are online at
  www.techzoom.net/risk

Research sponsored by

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Swiss Federal Institute of Technology, Zurich
www.csg.ethz.ch

References

Security Information Providers

- www.cert.org CERT
- www.secunia.com Secunia
- www.frsirt.com FrSirt
- www.iss.net ISS Internet Security Systems
- www.securityfocus.com SecurityFocus

Vulnerability Databases

- www.nvd.nist.gov National Vulnerability Database
- www.osvdb.org Open Source Vulnerability Database

Misc

- www.csg.ethz.ch Swiss Federal Institute of Technology, ComSys Group
- www.techzoom.net/risk Dynamics of Insecurity online
- en.wikipedia.org/wiki/Cumulative_distribution_function Statistics