



# 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>

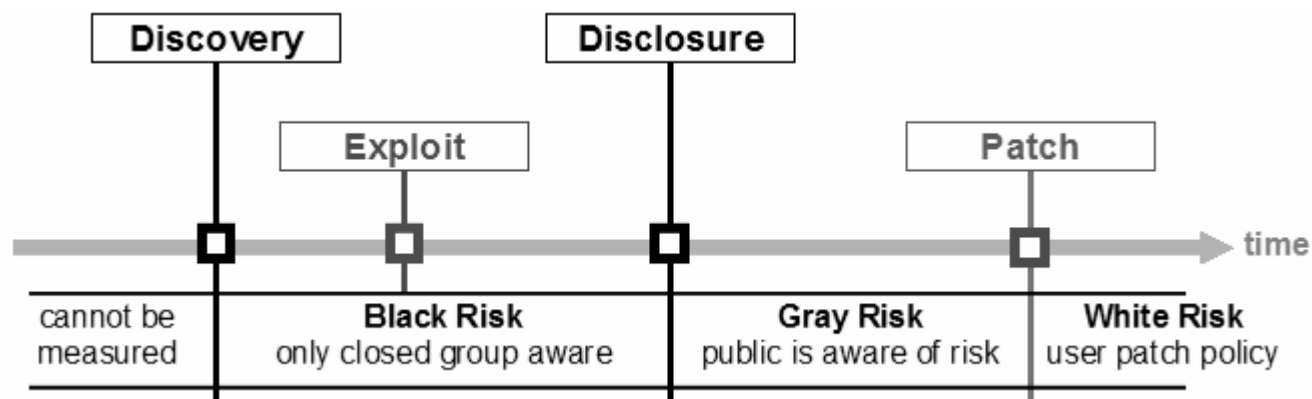
<http://www.techzoom.net/risk>



Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

# Vulnerability lifecycle

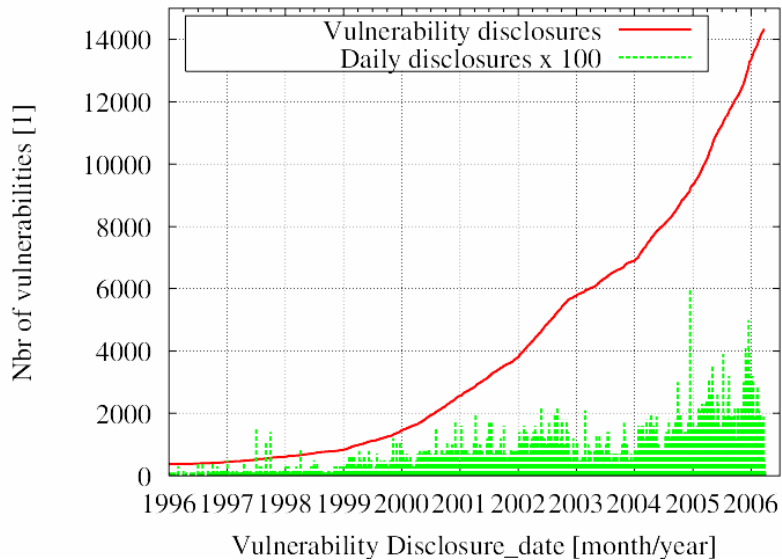
Exploring the vulnerability lifecycle ..



.. for all vulnerabilities with a CVE

- discovery, disclosure, exploit, and patch date

# Data and analysis



Exploring known vulnerabilities from 1996-2006

Vulnerability data from NVD, OSVDB

Problem: Lifecycle data?

## Analysis of

- examined security information providers > disclosure date
- 14,000+ vulnerabilities with a CVE
- 80,000+ security advisories

## What is the disclosure-date?

- first discussion of a potential vulnerability in a security list?
- vague 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

# Security Information Providers

## Potential providers for the disclosure-date

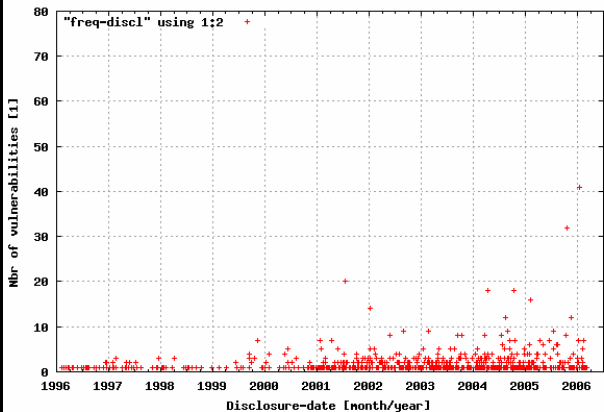
- **CERT** (Computer Emergency Response Team, USA)  
[www.cert.org](http://www.cert.org), started before 1996
- **Secunia** (Secunia, Denmark)  
[www.secunia.com](http://www.secunia.com), since 2002
- **FrSirt** (French Security Incident Response Team, France)  
[www.frSirt.com](http://www.frSirt.com),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

# Candidates to provide the disclosure-date

Number of vulnerabilities disclosed per day from 1996-2006

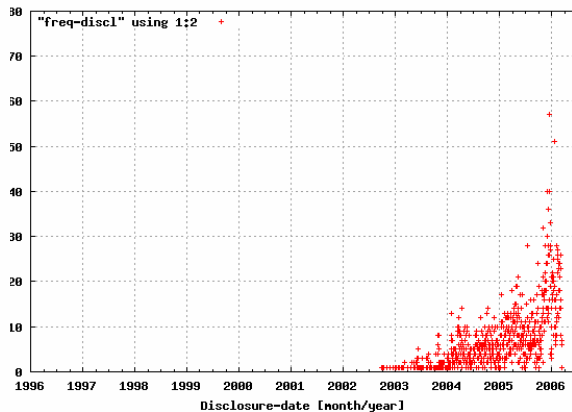
## Cert

Vulnerability count vs Disclosure-date  
absolute values  
(727 points/1410 events) 20060330 15:38.31



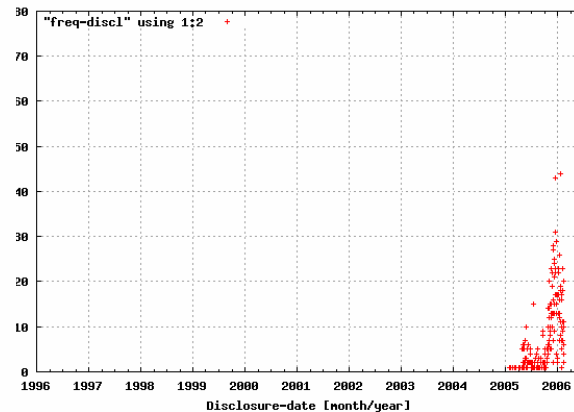
## Secunia

Vulnerability count vs Disclosure-date  
absolute values  
(652 points/4841 events) 20060330 15:30.13



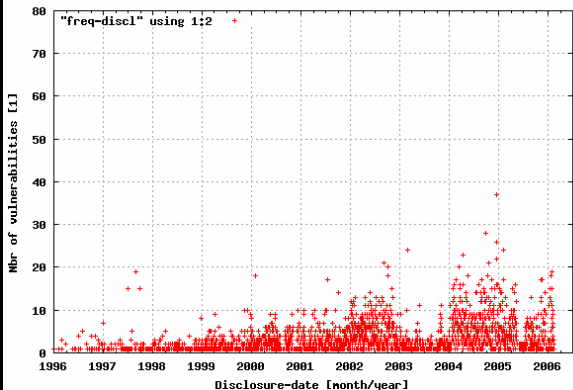
## FrSirt

Vulnerability count vs Disclosure-date  
absolute values  
(170 points/1425 events) 20060330 15:32.59



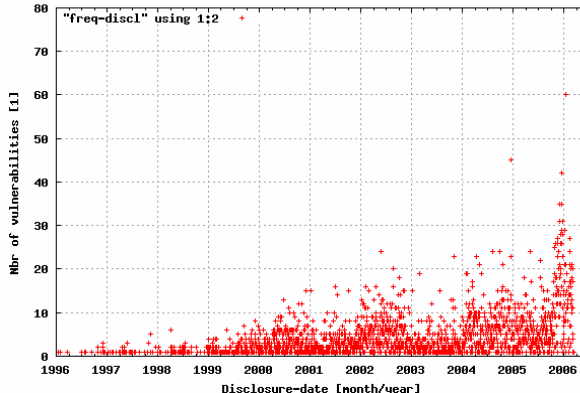
## ISS x-Force

Vulnerability count vs Disclosure-date  
absolute values  
(2178 points/8330 events) 20060330 15:26.56



## Securityfocus

Vulnerability count vs Disclosure-date  
absolute values  
(2163 points/10826 events) 20060330 15:24.00



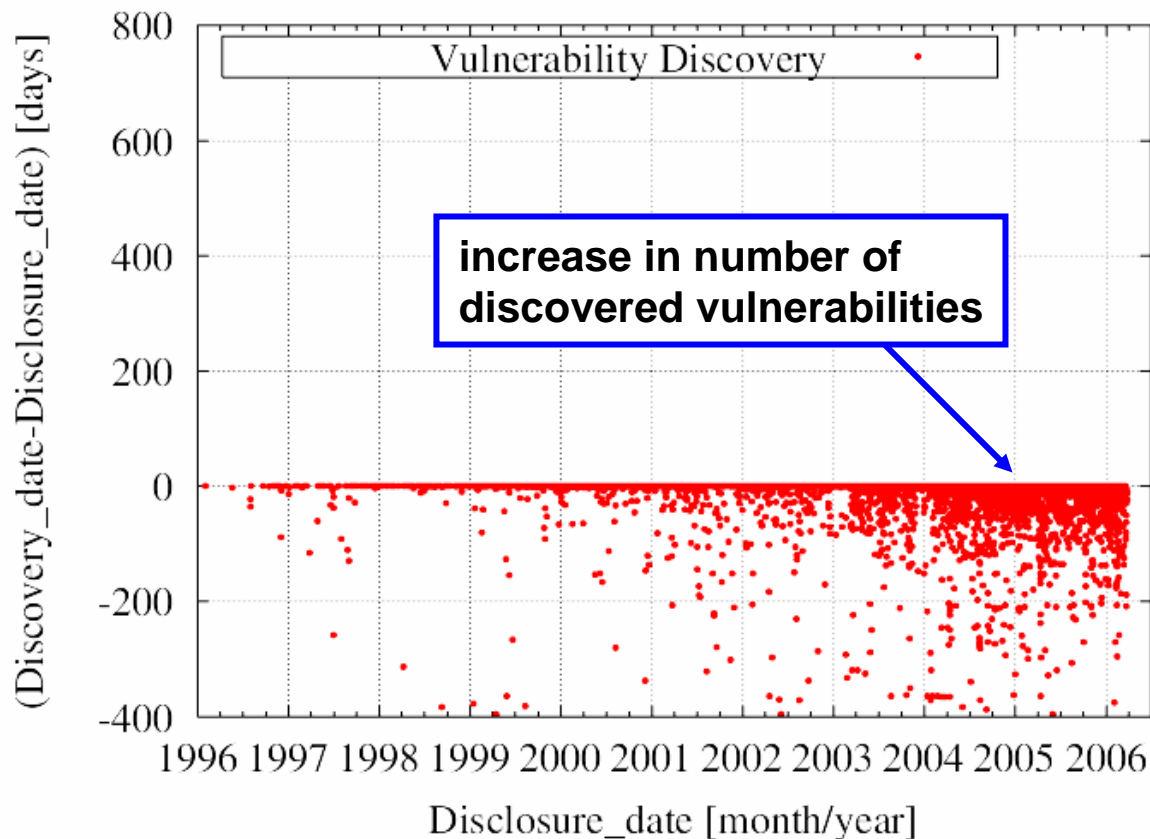
## ISS+Securityfocus:

- well established
- long history
- largest dataset

Secunia+FrSirt good for recent vulnerabilities

# Discovery-date Analysis

## Discovery-date vs disclosure-date



**Y-Axis:**  
days between **discovery-**  
**and disclosure-date** in  
days

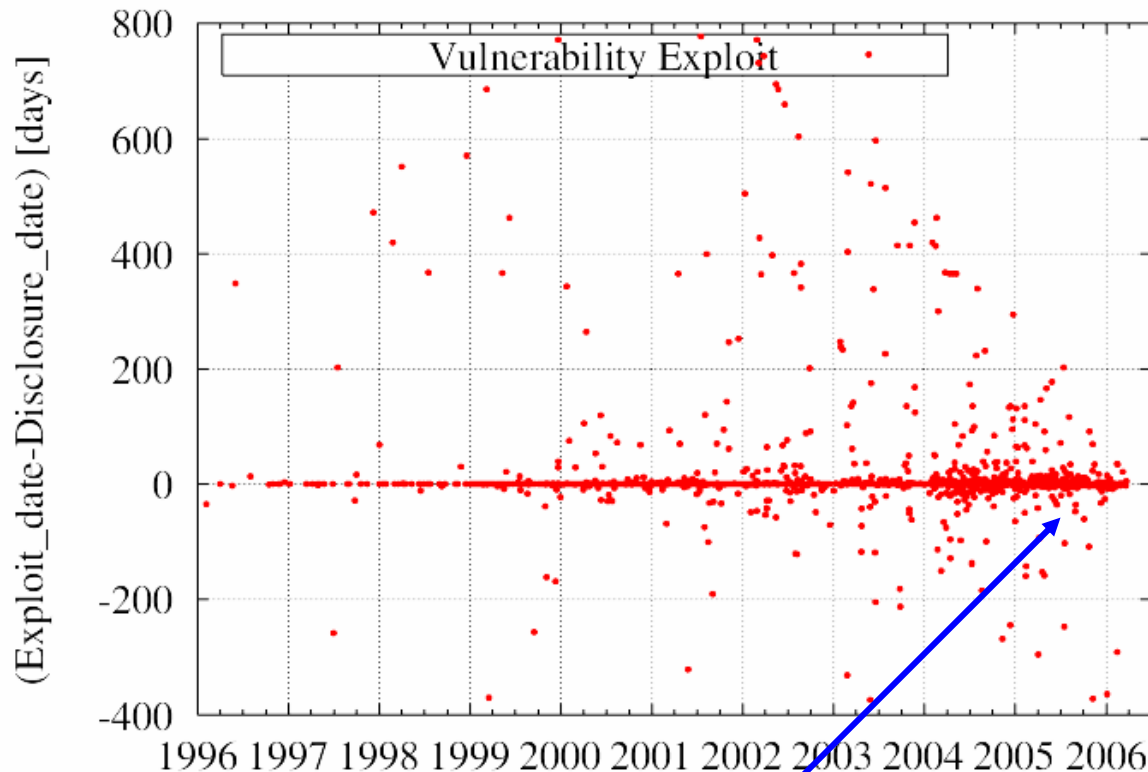
**X-Axis:**  
**disclosure-date**

**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

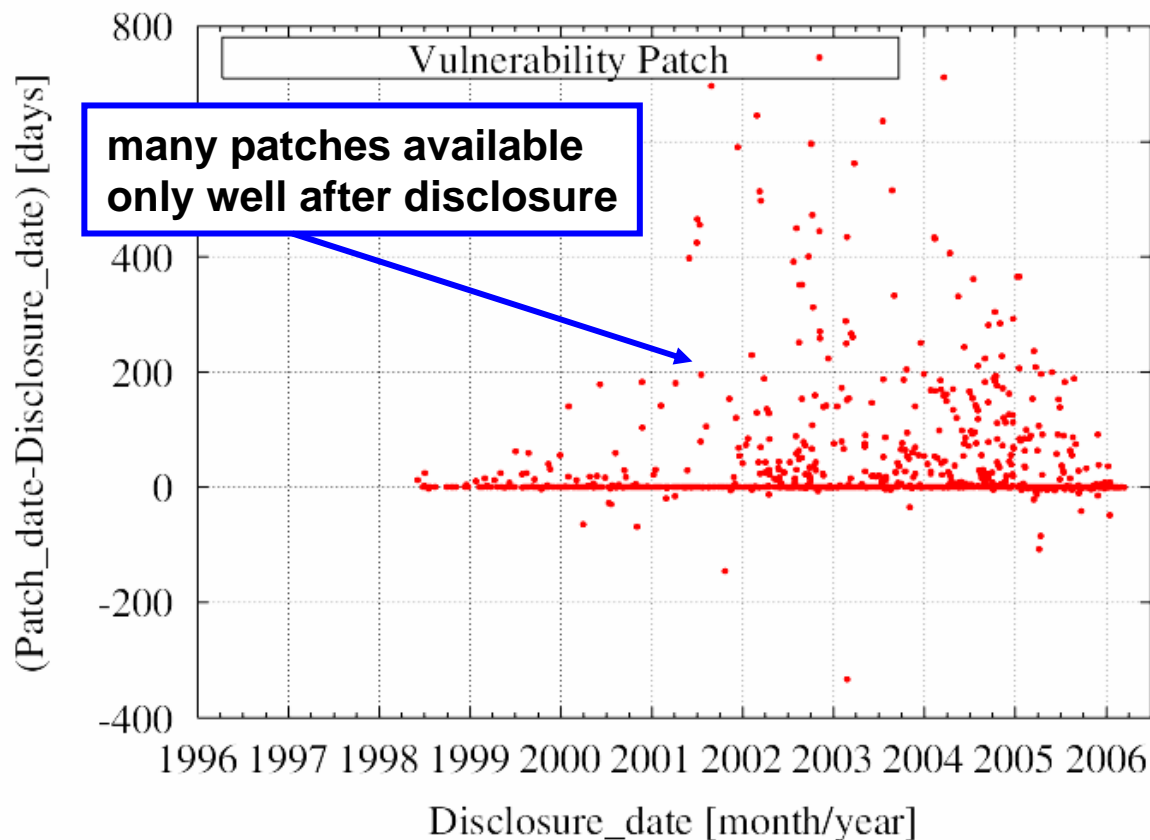
- 23% before disclosure

- 58% at disclosure

- 19 % after disclosure

# Patch Availability

## Patch availability date vs disclosure-date



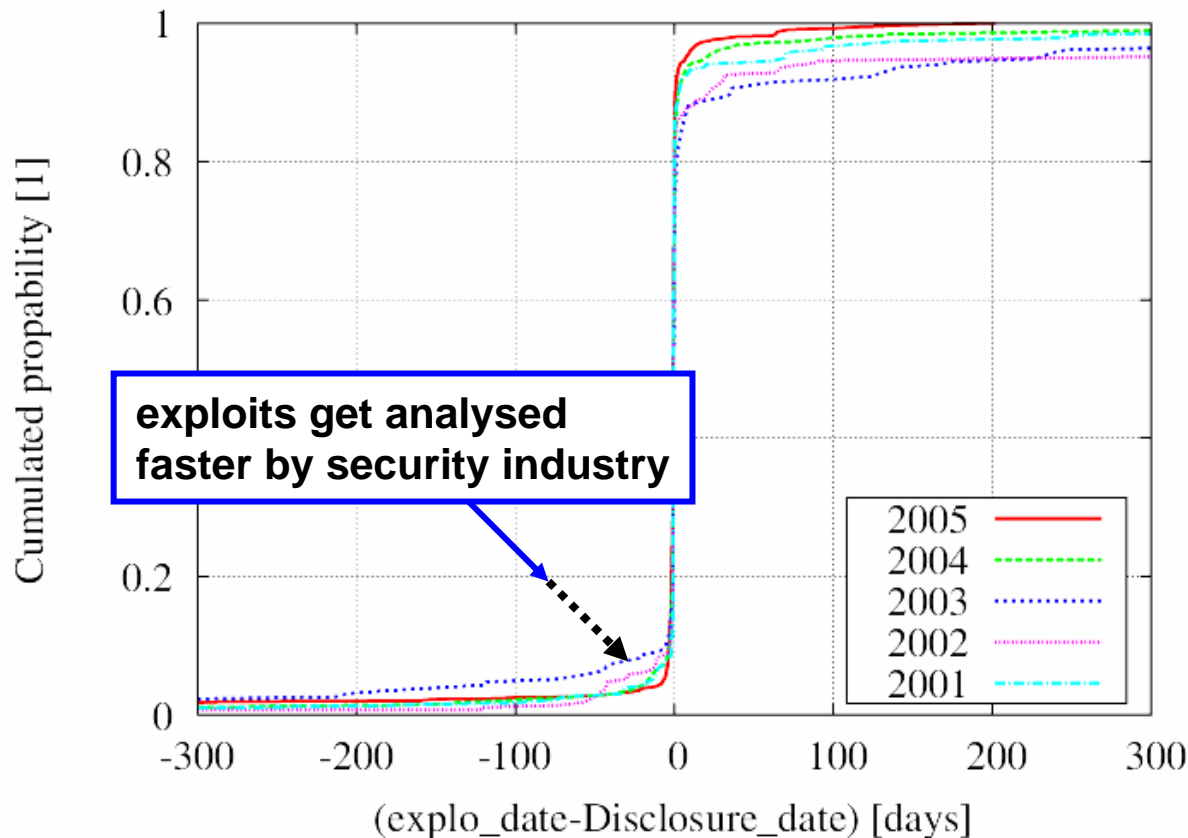
**Y-Axis:**  
days between **patch-** and **disclosure-date** in days

**X-Axis:**  
**disclosure-date**

**Data**  
-1551 patches

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

# Speed of Insecurity – Exploit availability

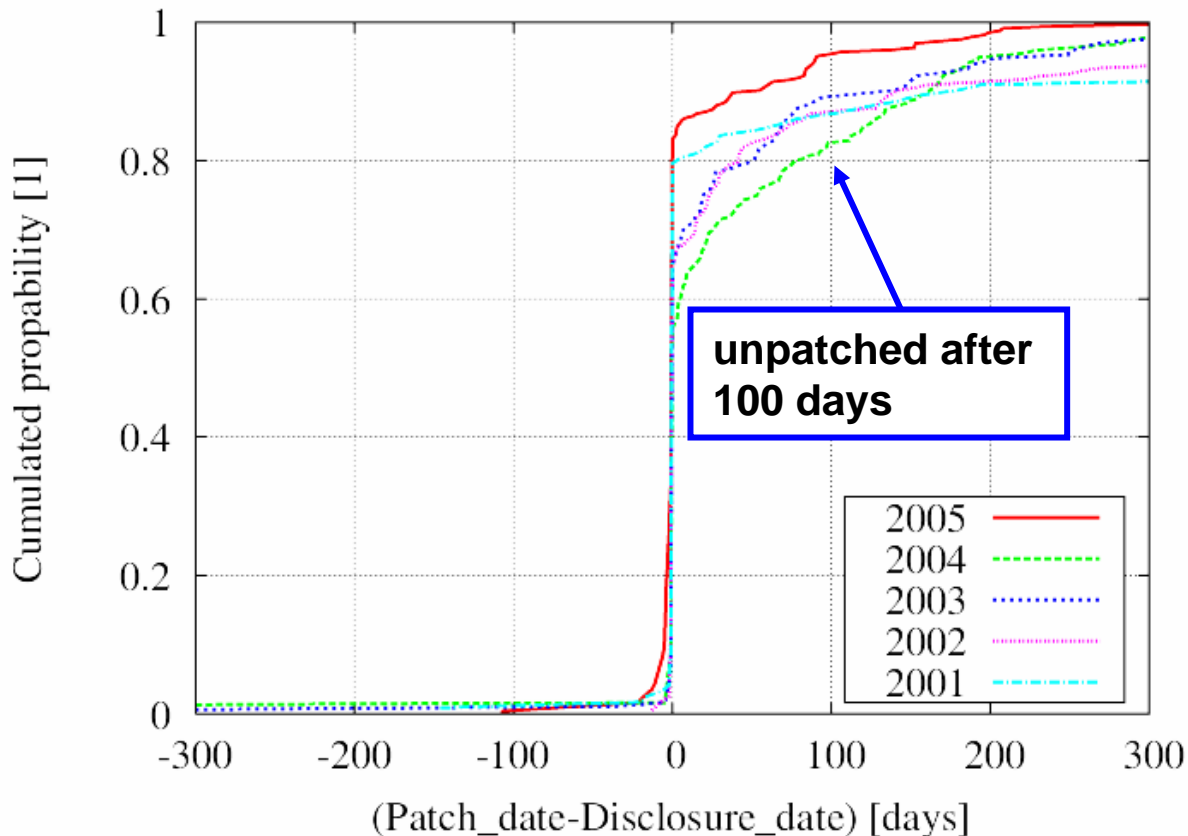


**Y-Axis:**  
cumulated probability  
for **exploit dates 2001-2005**

**X-Axis:**  
**days from disclosure-date**

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

# Speed of Security – Patch availability

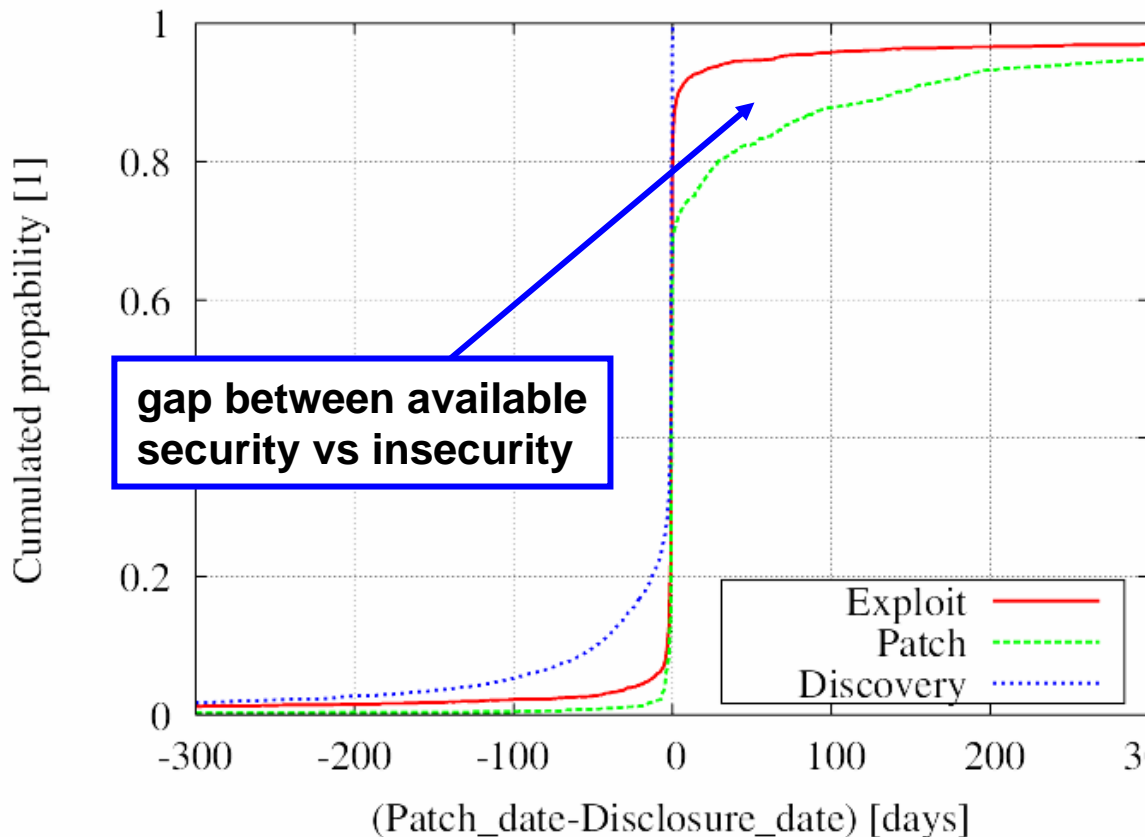


**Y-Axis:**  
cumulated probability  
for **patch-dates 2001-**  
**2005**

**X-Axis:**  
**days from disclosure-**  
**date**

# The Speed of (In)security

## The dynamics of security vs insecurity



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

**X-Axis:**  
**days from disclosure-**  
**date**

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

## Conclusion

- first analysis of relation between patch- and exploit-dates on this scale
- large dataset (14,000+ vulnerabilities, 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](http://www.techzoom.net/risk)

# Thank you

- All plots are online at [www.techzoom.net/risk](http://www.techzoom.net/risk)
- Technical Paper at SIGCOMM Workshop 11-Sep-06, Pisa, Italy
- Feedback and comments highly appreciated

Research sponsored by



Eidgenössische Technische Hochschule Zürich  
Swiss Federal Institute of Technology Zurich

Swiss Federal Institute of Technology, Zurich  
[www.csg.ethz.ch](http://www.csg.ethz.ch)