0-Day Patch

Exposing vendors (in)security performance

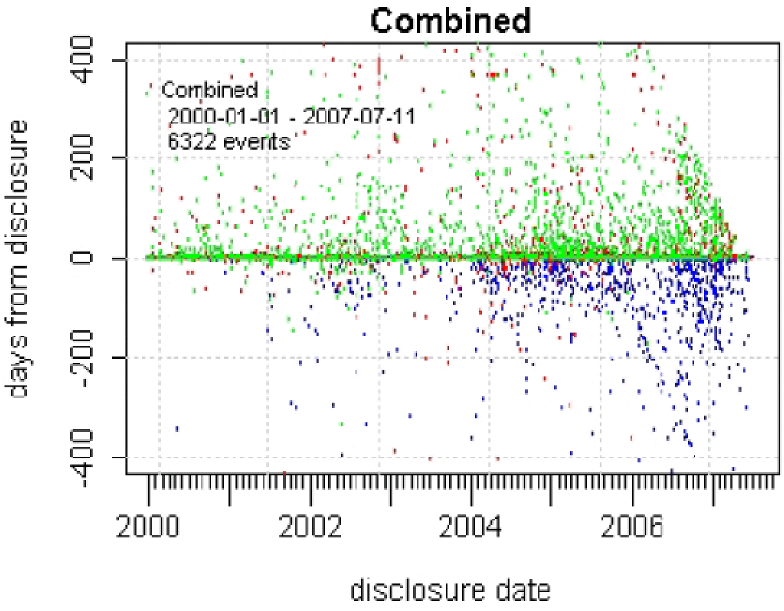
BlackHat Europe 2008 – Amsterdam

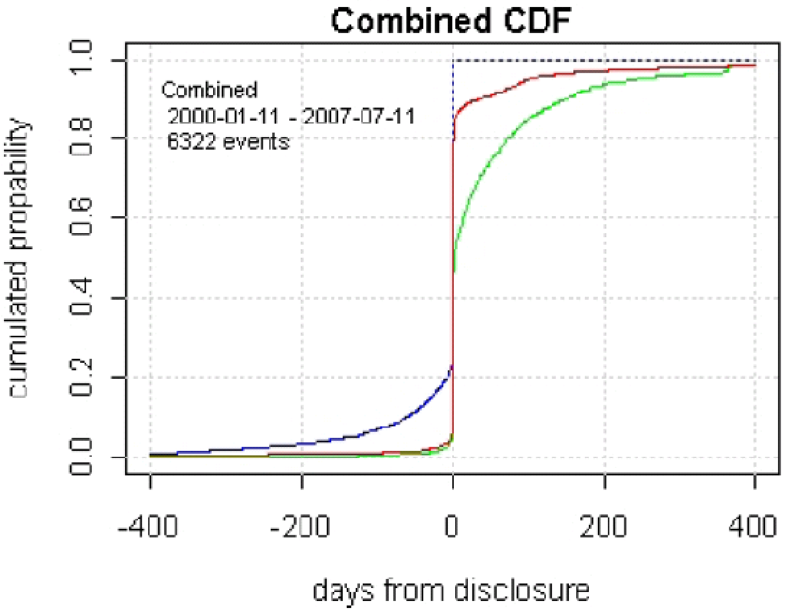
Stefan Frei + Bernhard Tellenbach
Communication Systems Group
ETH Zurich – Switzerland
http://www.csg.ethz.ch
http://www.techzoom.net/risk

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Evolution of the Security Ecosystem

- What is the performance of software vendors?
- How many patches available at 0-Day?
- Does responsible disclosure really work?
- Global trends vs. vendor specific issues

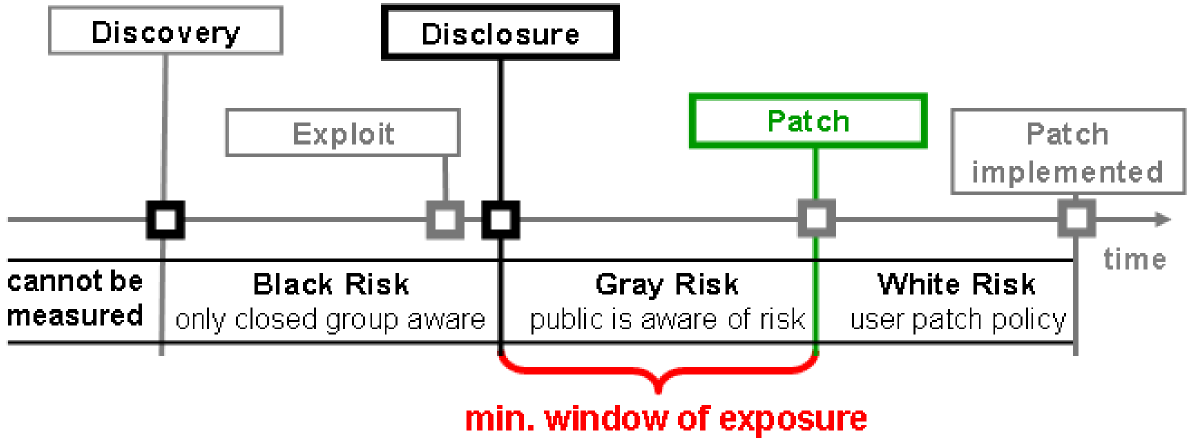




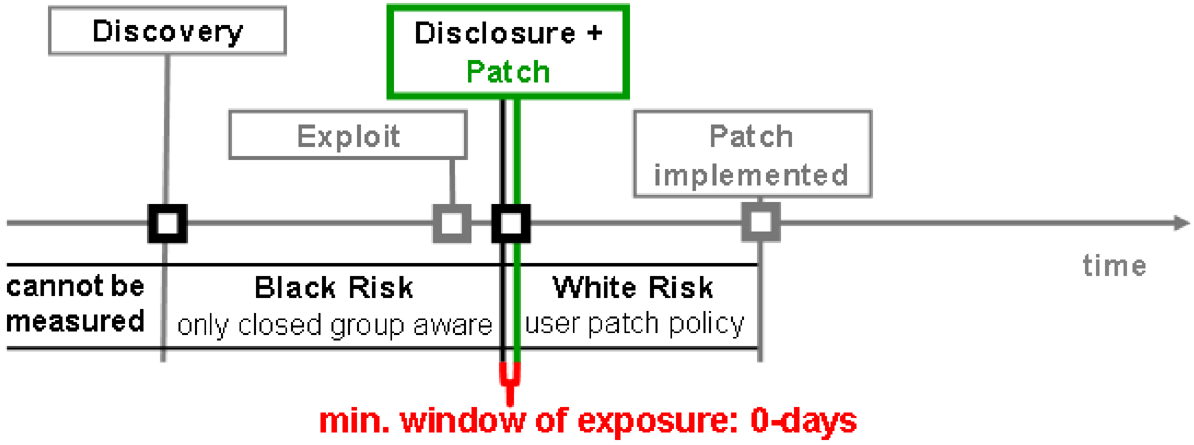
What is a 0-Day Patch?

- Lifecycle of a vulnerability - exposure time

Non-0-Day Patch



0-Day Patch



What is the Disclosure-Date?

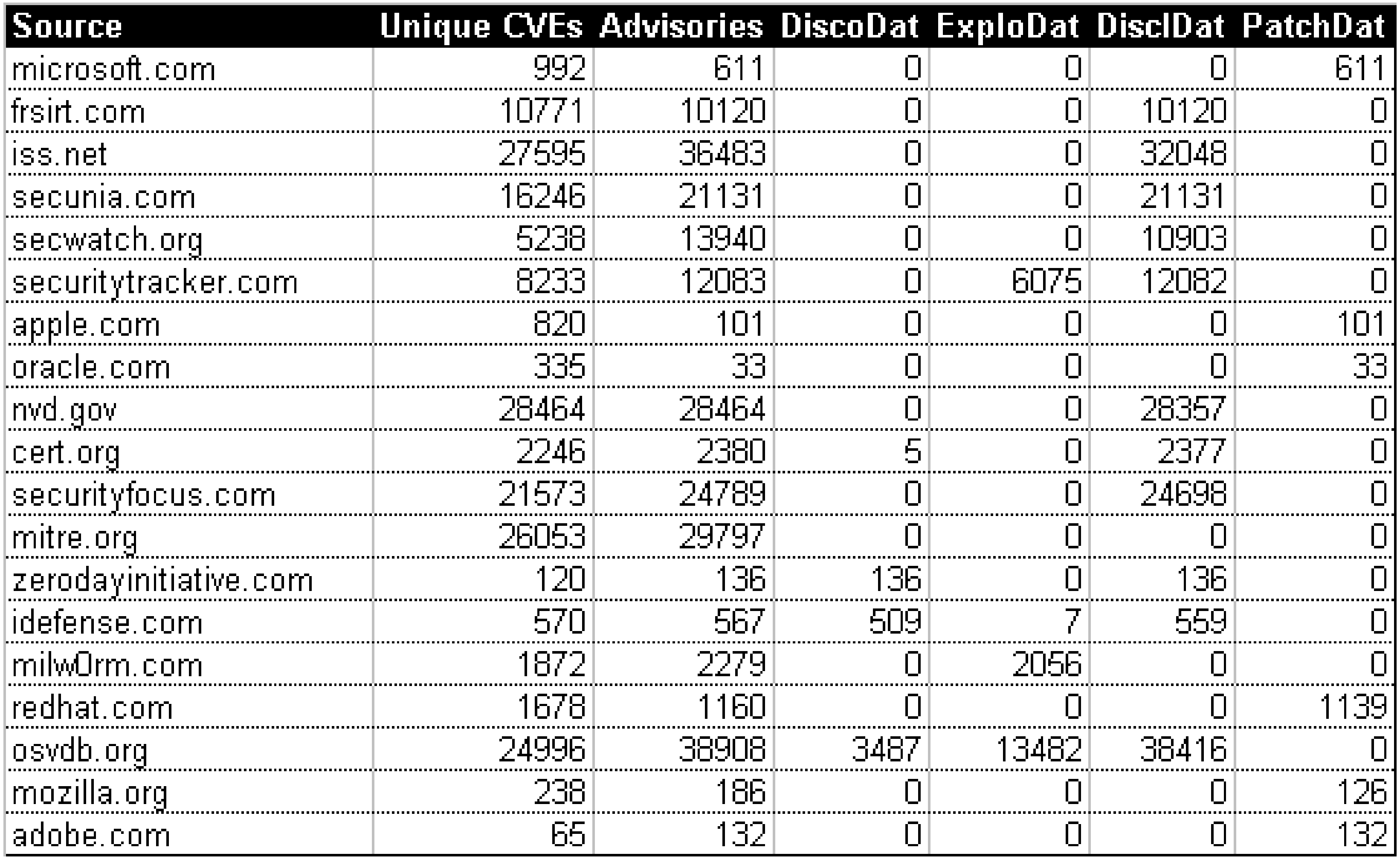
Our requirements:

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

→ **Disclosure-Date of a vulnerability:**

Date of the first advisory issued
by a trusted and independent source

Data Sources



Source	Unique CVEs	Advisories	DiscoDat	ExploDat	DisclDat	PatchDat
microsoft.com	992	611	0	0	0	611
frsirt.com	10771	10120	0	0	10120	0
iss.net	27595	36483	0	0	32048	0
secunia.com	16246	21131	0	0	21131	0
secwatch.org	5238	13940	0	0	10903	0
securitytracker.com	8233	12083	0	6075	12082	0
apple.com	820	101	0	0	0	101
oracle.com	335	33	0	0	0	33
nvd.gov	28464	28464	0	0	28357	0
cert.org	2246	2380	5	0	2377	0
securityfocus.com	21573	24789	0	0	24698	0
mitre.org	26053	29797	0	0	0	0
zerodayinitiative.com	120	136	136	0	136	0
idefense.com	570	567	509	7	559	0
milw0rm.com	1872	2279	0	2056	0	0
redhat.com	1678	1160	0	0	0	1139
osvdb.org	24996	38908	3487	13482	38416	0
mozilla.org	238	186	0	0	0	126
adobe.com	65	132	0	0	0	132

0-Day patch: Overall performance

Interpretation of plots

- 0-Day patch rate since 2002
- For High and Medium risk vulnerabilities patched till Dec 2007
- Sliding window, 360 days
- Green (0-day patch) measures share of the responsible disclosure process
- Blue+Red measure the performance of vendor to produce a patch in 30 or 90 days
- Grey, do we ever get a patch? (ever = in less than 180 days)

Y-Axis:

Fraction of vulnerabilities patched in less than:

🟩 1 day (0-day)
🟦 30 days
🟥 90 days
▬ 180 days

after disclosure

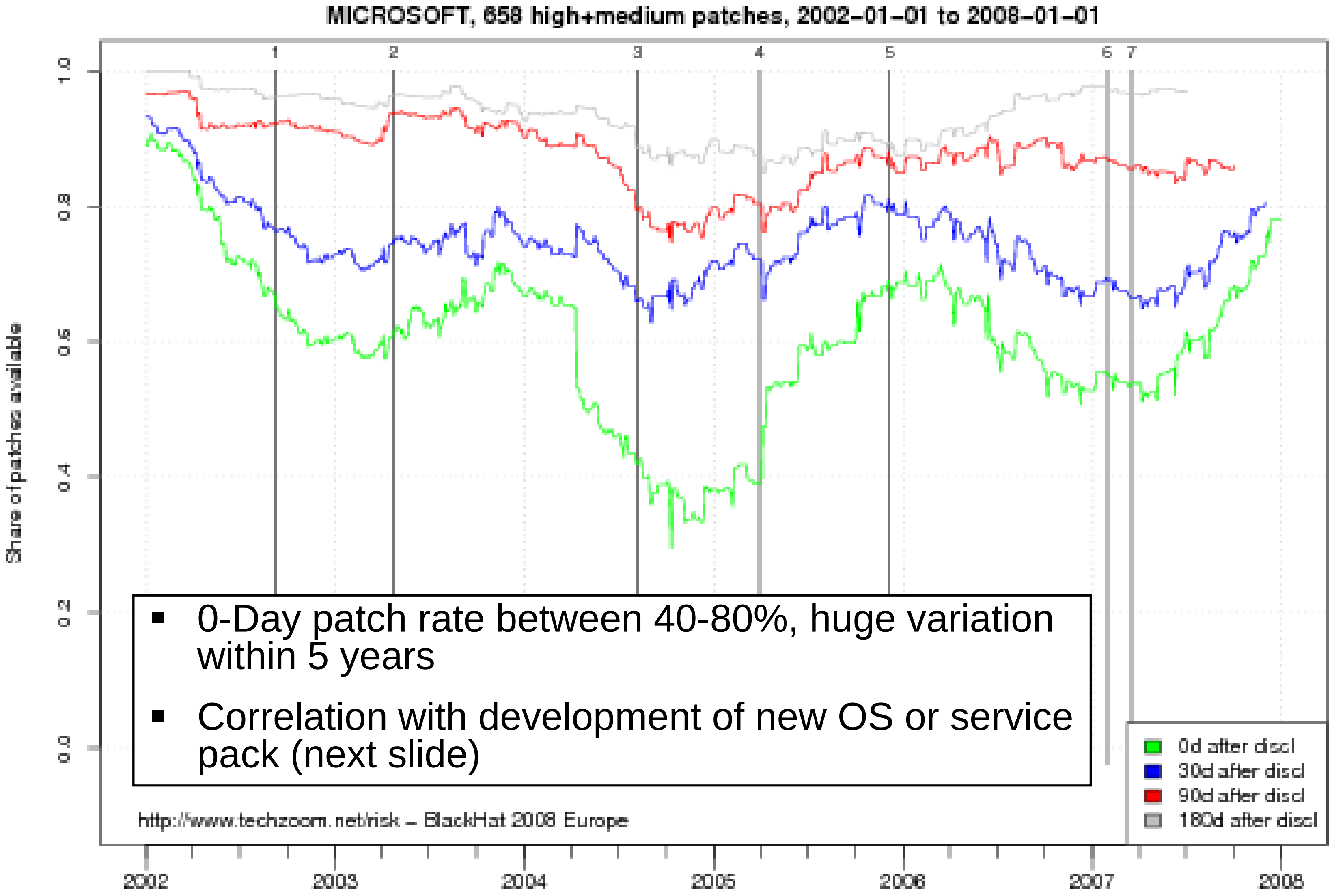
X-Axis:

time (years)

# **Vulnerabilities** patched between 2002-2008

Apple: 738
Microsoft: 658

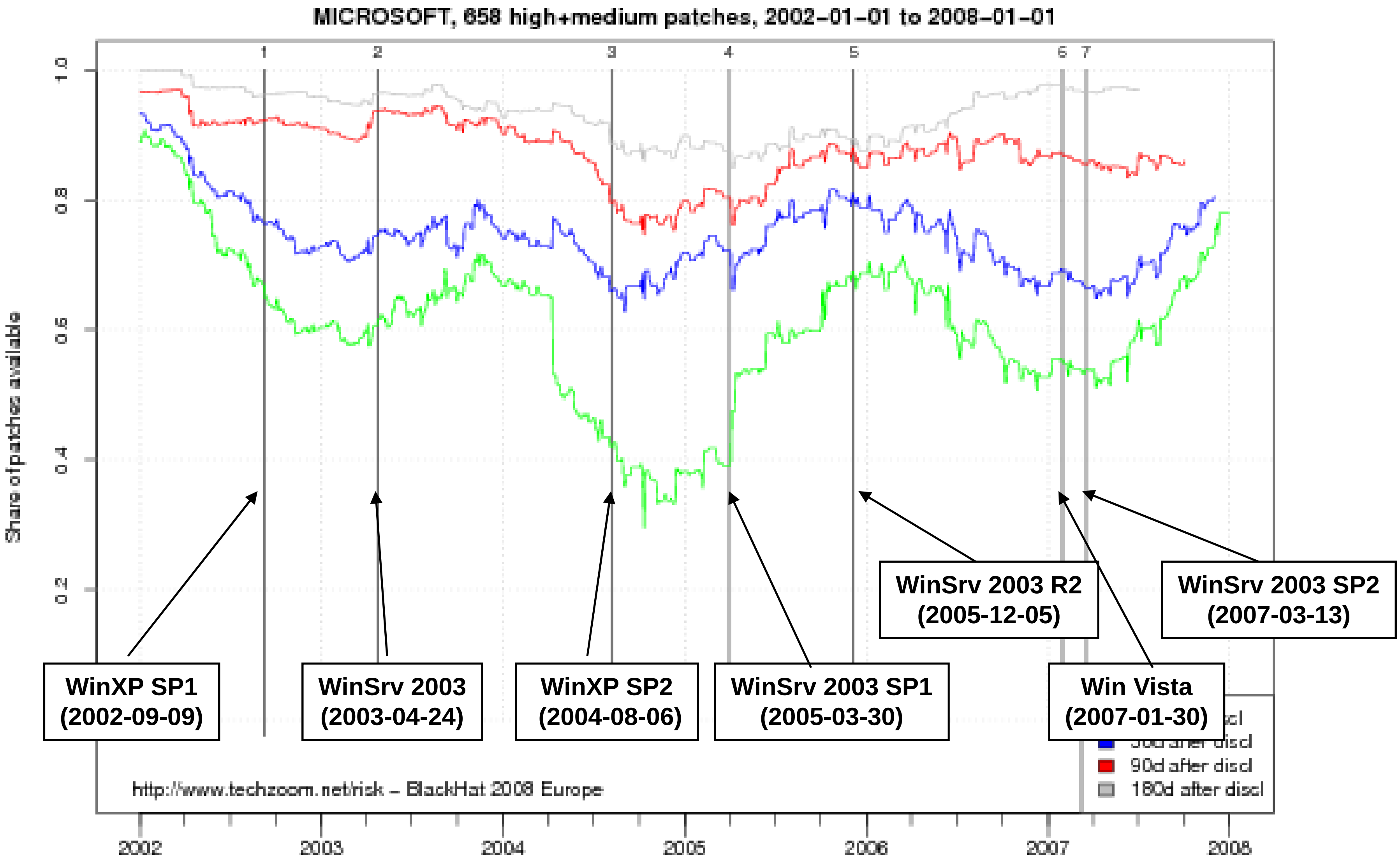
0-Day Patch: Microsoft



- 0-Day patch rate between 40-80%, huge variation within 5 years
- Correlation with development of new OS or service pack (next slide)

http://www.techzoom.net/risk – BlackHat 2008 Europe

0-Day Patch: Microsoft



WinXP SP1
(2002-09-09)

WinSrv 2003
(2003-04-24)

WinXP SP2
(2004-08-06)

WinSrv 2003 SP1
(2005-03-30)

WinSrv 2003 R2
(2005-12-05)

Win Vista
(2007-01-30)

WinSrv 2003 SP2
(2007-03-13)

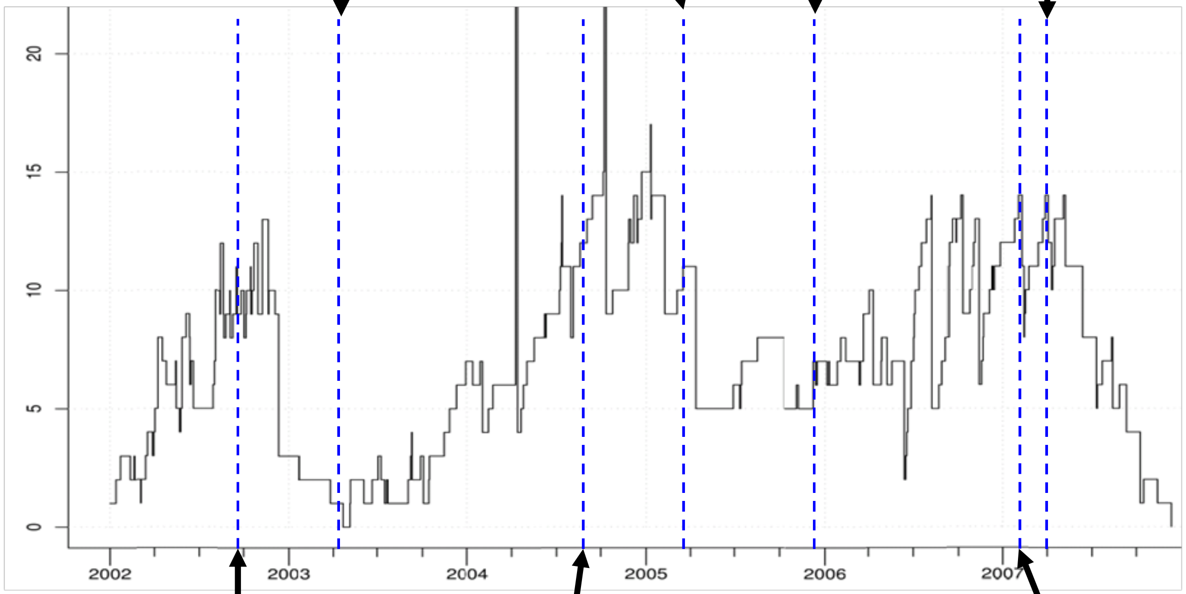
of Unpatched Vulnerabilities: Microsoft

Win Server 2003 SP1
(March 30, 2005)

Win Server 2003 SP2
(March 13, 2007)

Win Server 2003
(April 24, 2003)

Win Server 2003 R2
(December 6, 2005)



WinXP SP1
(September 9, 2002)

WinXP SP2
(August 6, 2004)

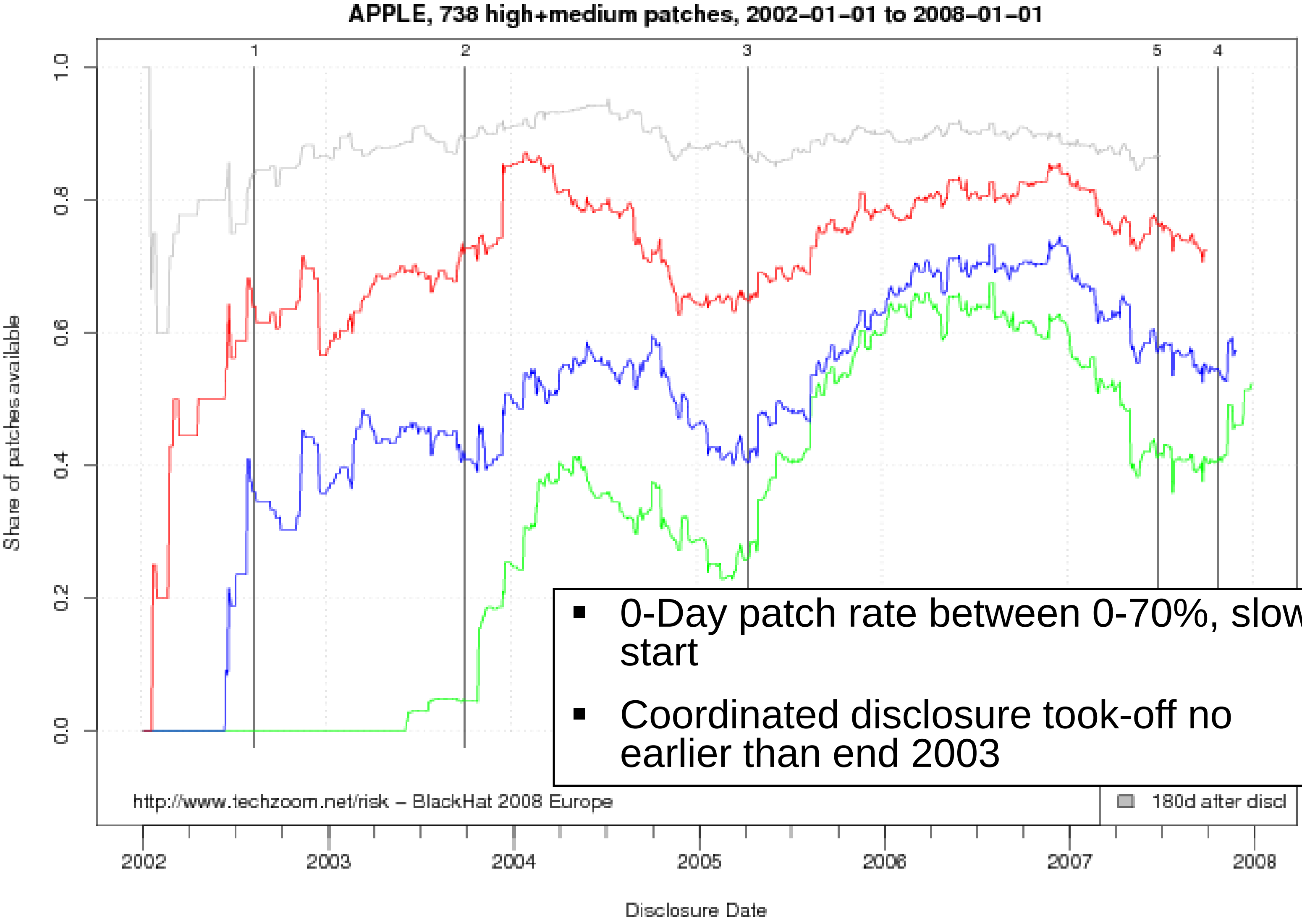
Win Vista
(January, 30, 2007)

Y-Axis:
Number of unpatched vulnerabilities

X-Axis:
time (years)

- Evolution of the number of unpatched vulnerabilities at a certain date

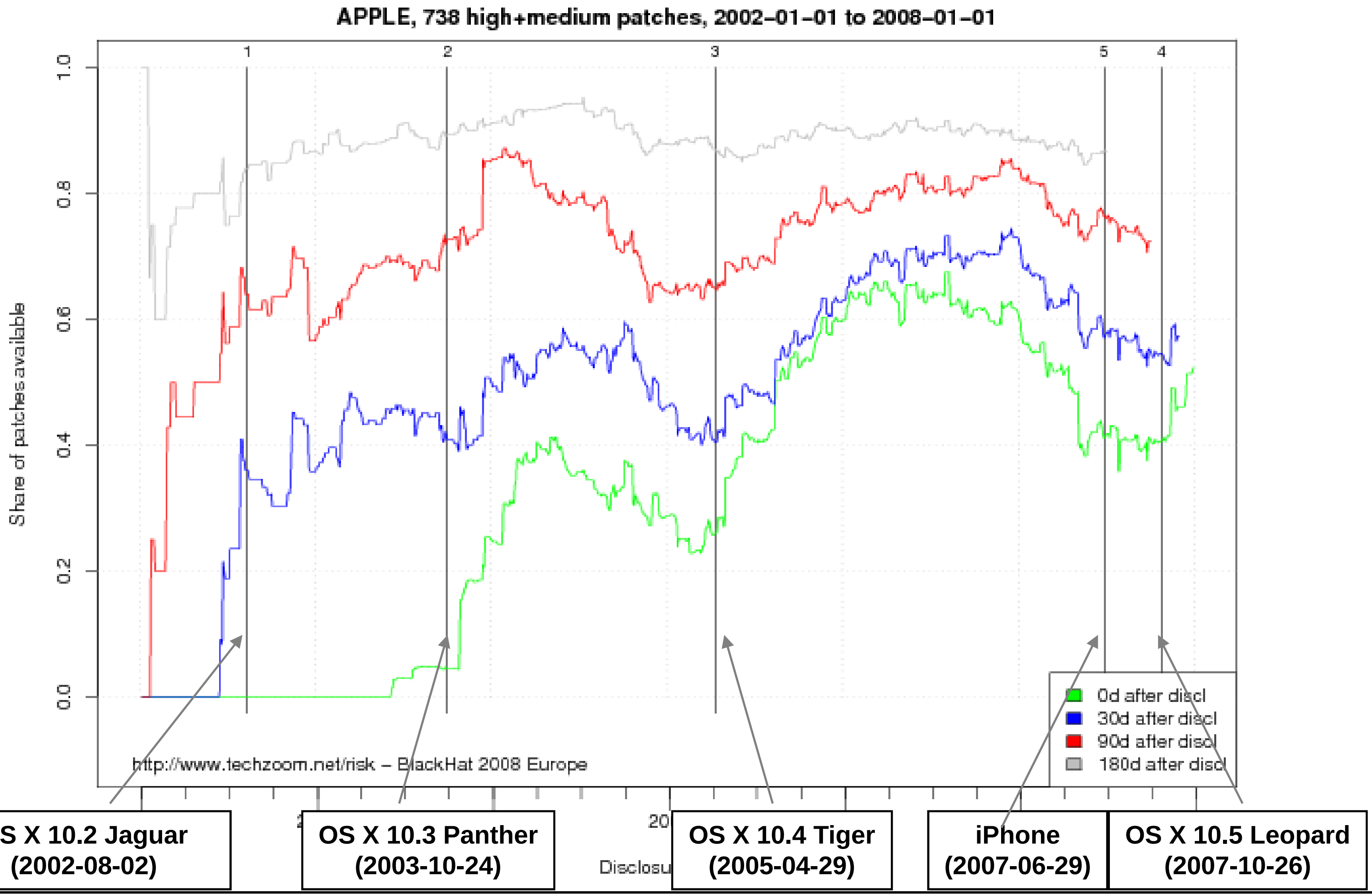
0-Day Patch: Apple



- 0-Day patch rate between 0-70%, slow start
- Coordinated disclosure took-off no earlier than end 2003

BLACKHAT Europe 2008 – 0-Day Patch

0-Day Patch: Apple



OS X 10.2 Jaguar (2002-08-02)

OS X 10.3 Panther (2003-10-24)

OS X 10.4 Tiger (2005-04-29)

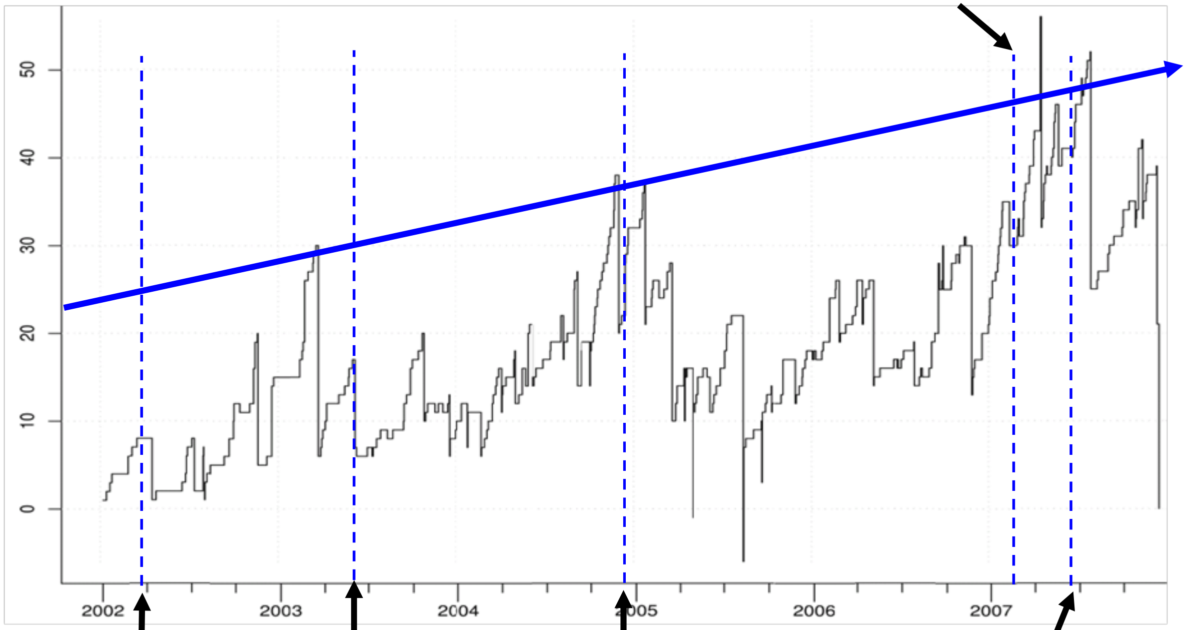
iPhone (2007-06-29)

OS X 10.5 Leopard (2007-10-26)

Unpatched Vulnerabilities: Apple

Apple

i-Phone release (USA)
(June 29, 2007)



OSX 10.3 “Panther“
(October 23, 2003)

OSX 10.4 “Tiger“
(April 29, 2005)

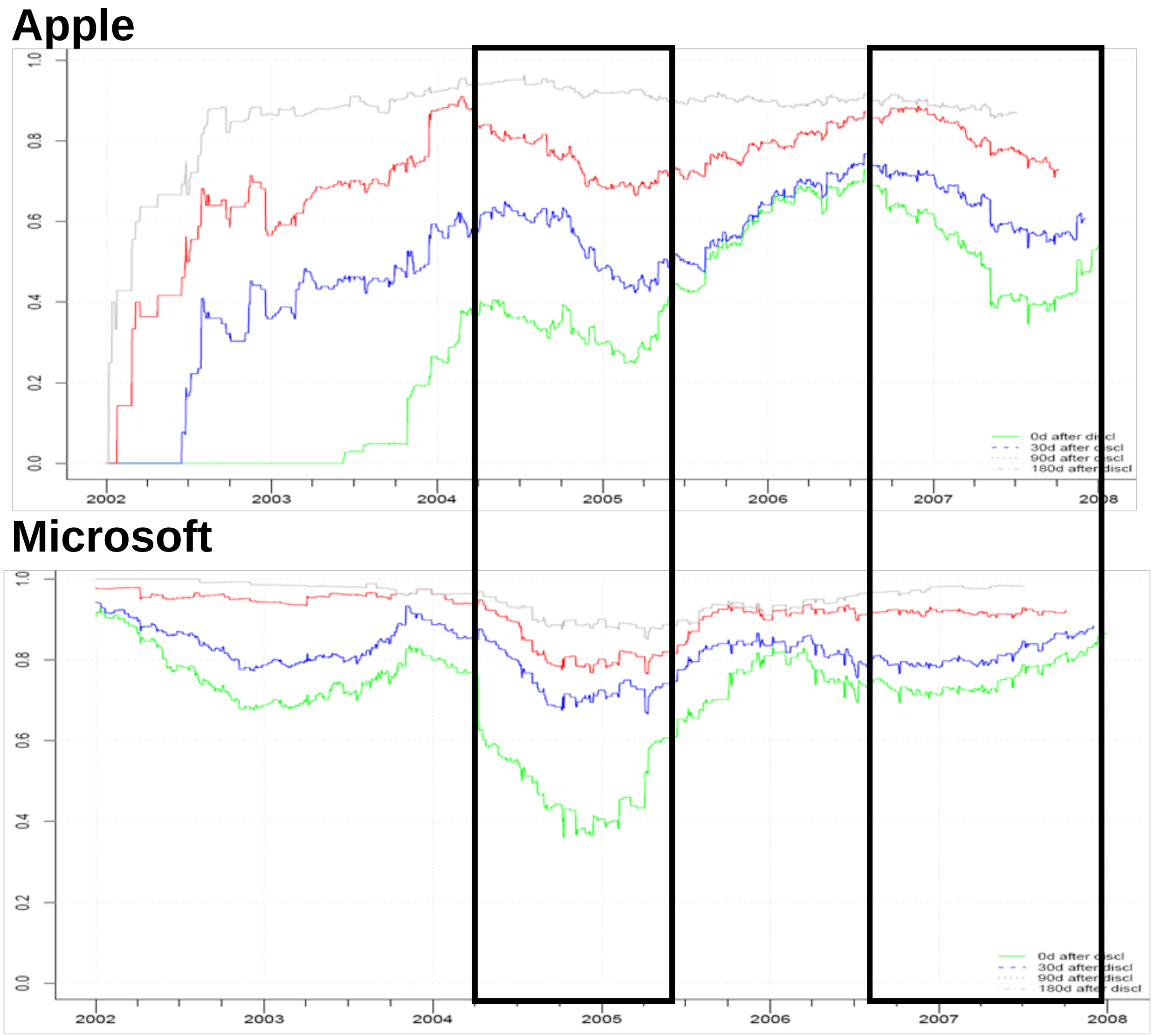
OSX 10.5 “Leopard“
(October 26, 2007)
delayed due to i-Phone

Y-Axis:
Number of unpatched vulnerabilities

X-Axis:
time (years)

- Evolution of the number of unpatched vulnerabilities at a certain date

High- and Medium Risk Patches: Apple vs. Microsoft



Y-Axis:

Fraction of vulnerabilities patched in less than:

🟩 1 day (0-day)

🟦 30 days

🟥 90 days

▬ 180 days

X-Axis:

time (years)

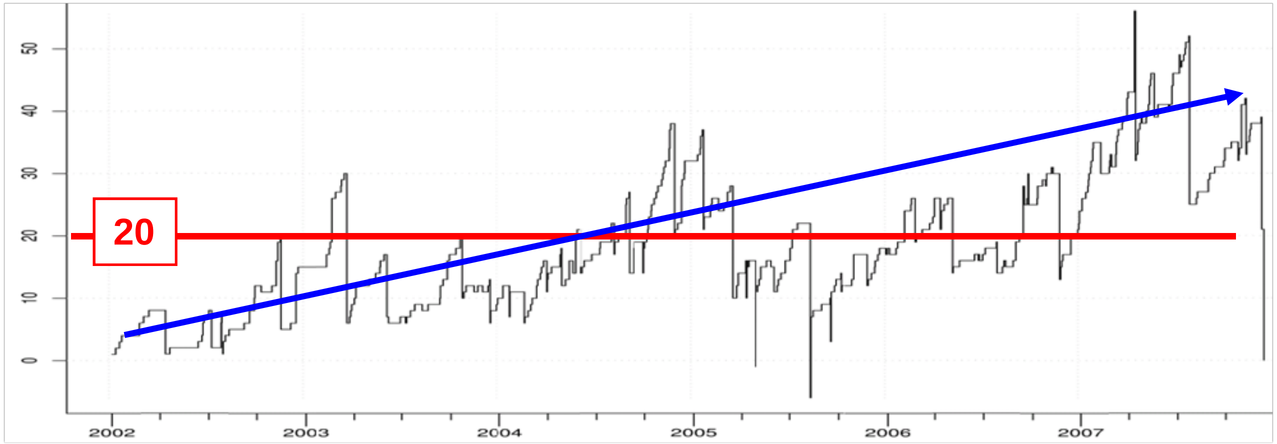
# Vulnerabilities

Apple: 738

Microsoft: 658

#Unpatched Vulnerabilities: Apple vs. Microsoft

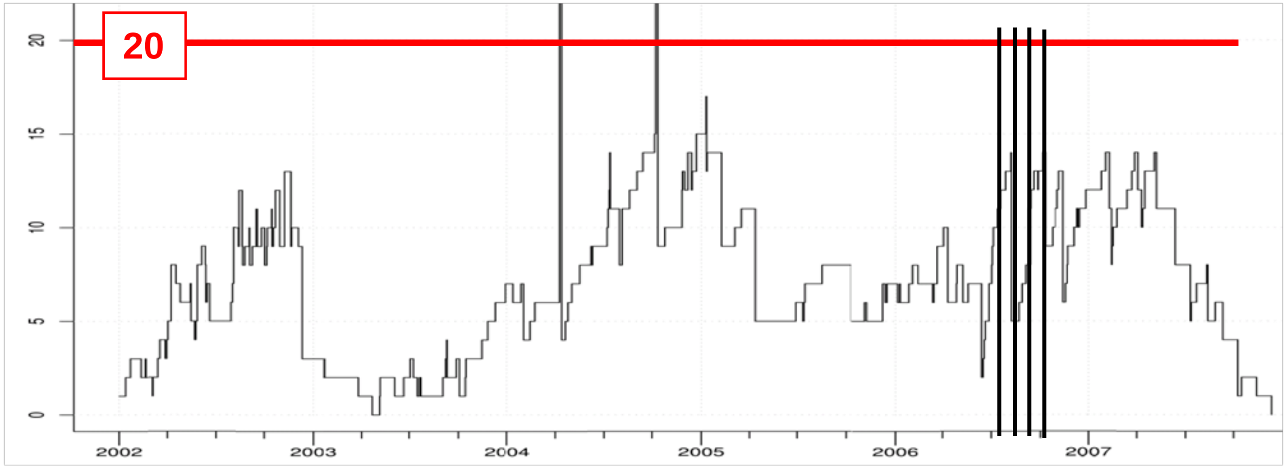
Apple



Y-Axis:
Number of unpatched vulnerabilities

X-Axis:
time (years)

Microsoft



# Unpatched Vulnerabilities
(Average)
Apple: increasing
Microsoft: stable

What does this mean?

- **High and medium risk**
  - Coordinated disclosure process is either at a high level (MS) or has increased considerably (Apple)
  - Fraction of vulnerabilities with 0-day patch is both surprisingly high and shockingly low over last 5 years
  - Service pack and OS development binds (security) resources

- **Number of concurrent unpatched vulnerabilities**
  - Microsoft: Remains in the same range (impacted by software lifecycle > devel. resources)
  - Apple: trend shows increasing number (to few resources to cope with side-effects of increased popularity of their products?)

Conclusion

- Introduction of 0-day patch as viable metric to measure the security processes of vendors
- Metric based on publicly available data
- First analysis of the 0-day (in)security performance of software vendors at this scale
- “Unbiased” data set by correlating information from multiple sources to antagonize possible bias in vendor information

Future

- Continued monitoring and database updates
- Implications and applications of these findings to security ecosystem and risk analysis models

Thank you

- All plots are online at `http://www.techzoom.net/risk`
- Feedback and comments highly appreciated

Research sponsored by

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

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