Ben Sapiro
Principal, Secure Applications & Systems

TELUS Security Solutions

Evolution of Technical Vulnerabilities

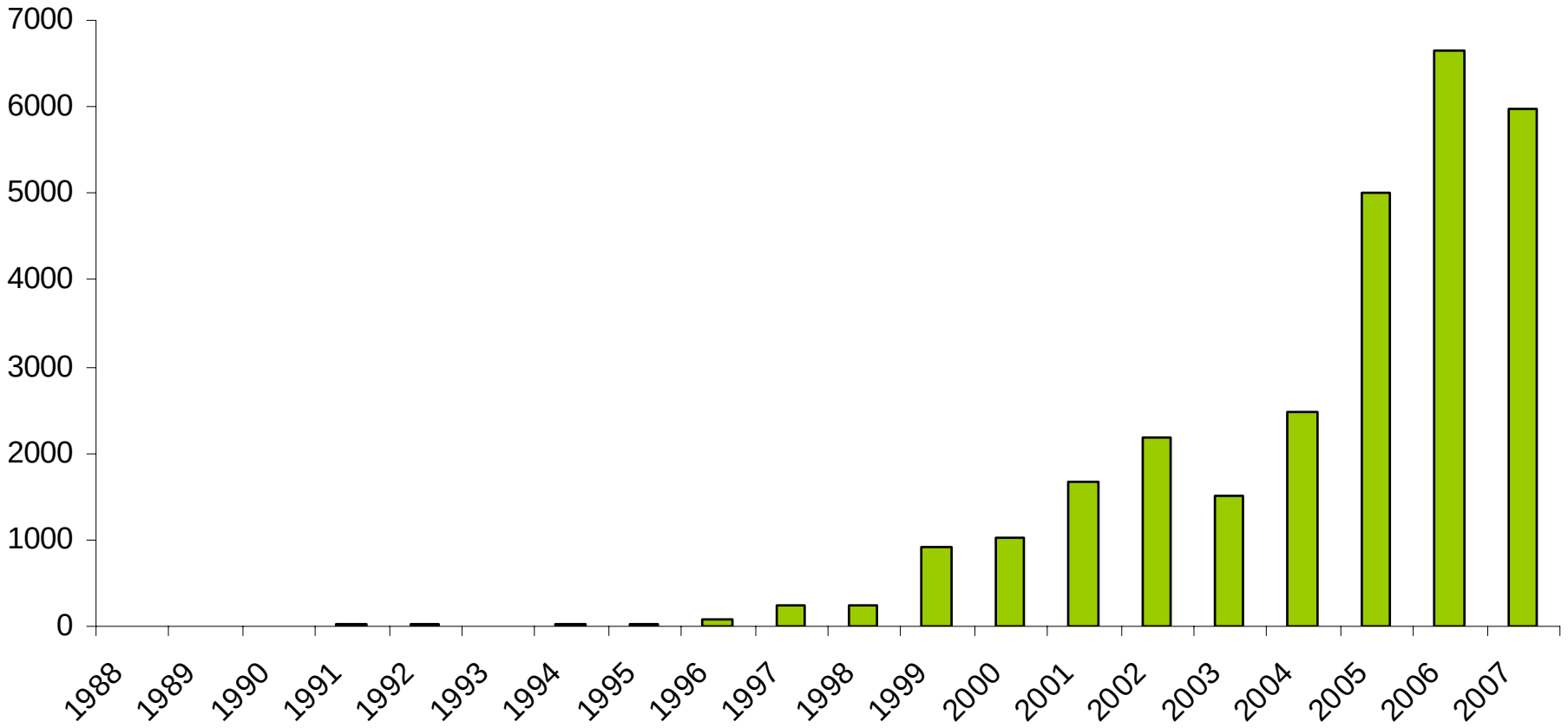
November, 2007

TELUS
the future is friendly®

Introductions

- Ben@TELUS
- TELUS does security?
- The origin of this talk

Vulnerability trends



Who has a crystal ball?

- Lots of analyst organizations are talking about emerging risks
  - Where are they buying their crystal balls?
- We have no crystal ball… but we have the next best thing
  - Extensive, private data source
  - Not publicly available
  - Used daily by most of the world's security product companies
  - National intelligence agencies
  - Global high-tech vendors
- We used that data source to hunt for trends in public sources

Assurent VR

- Provider of threat and vulnerability intelligence
  - Assurent Secure Technologies acquisition
  - Since Jan 2004
  - Daily technical data feeds on threats and vulnerabilities to:
    - ~50 security product vendors (including 17 of the top 20)
    - Global government intelligence agencies
    - High-tech manufacturers
    - Global financial services firms
    - Other global organizations
  - Power's NSS Labs' accuracy and coverage testing

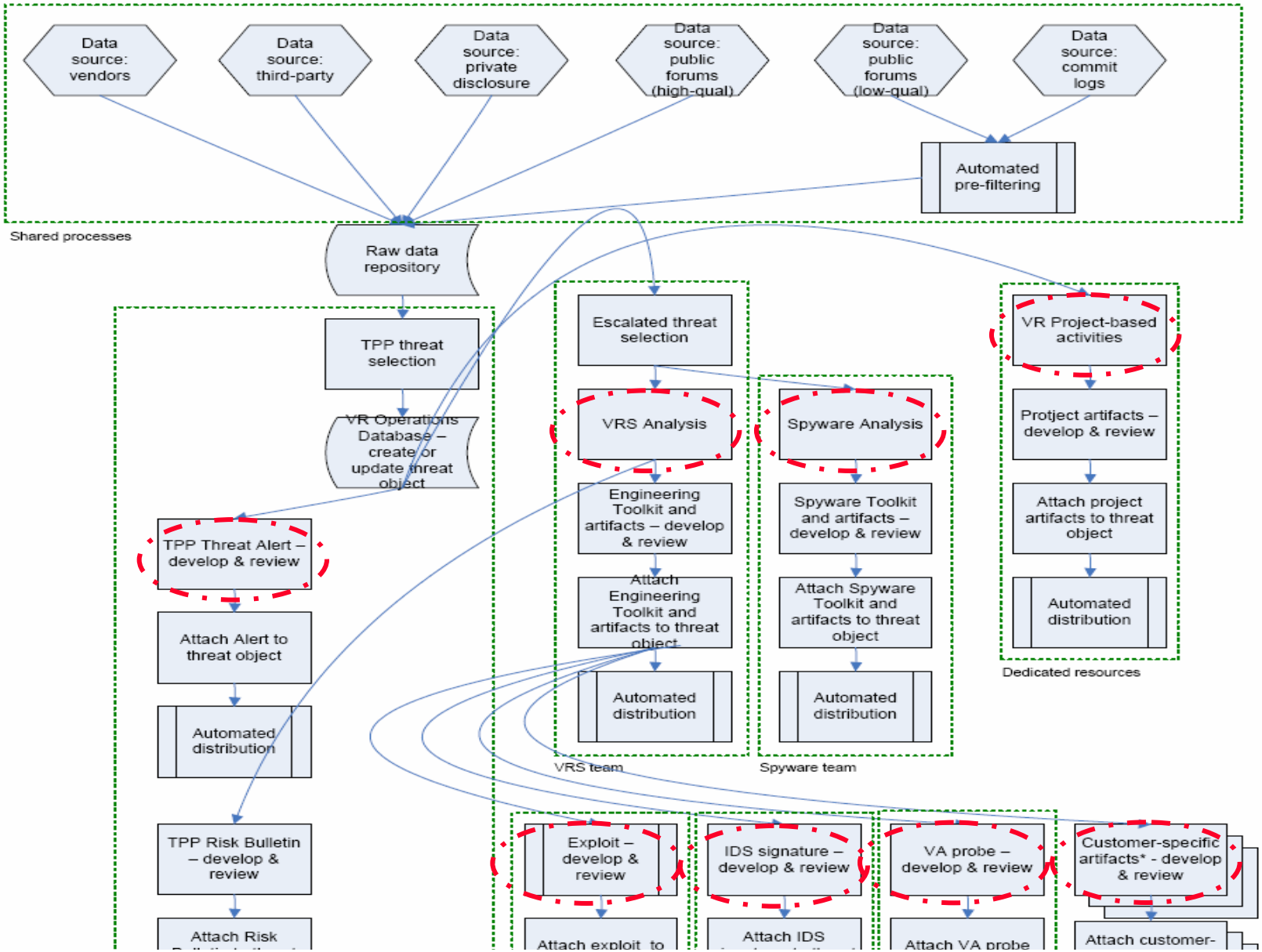
Assurent VR data streams

- **Vulnerability Research Engineering Report** (real-time feed & historical data)
- **Vulnerability and Exploit Signatures** (network- and host-based)
- **VA Probes feed**
- **Spyware Signatures** (real-time feed & historical data)
- **Shell Code Exploit** feed
- **Threat Protection Program** (advanced enterprise threat intelligence service)
- **Protocol Recognition Signatures**
- **Custom Artifact Feeds** for individual vendors (IPS signatures, VA probes, host-based checks, etc.)

Data produced

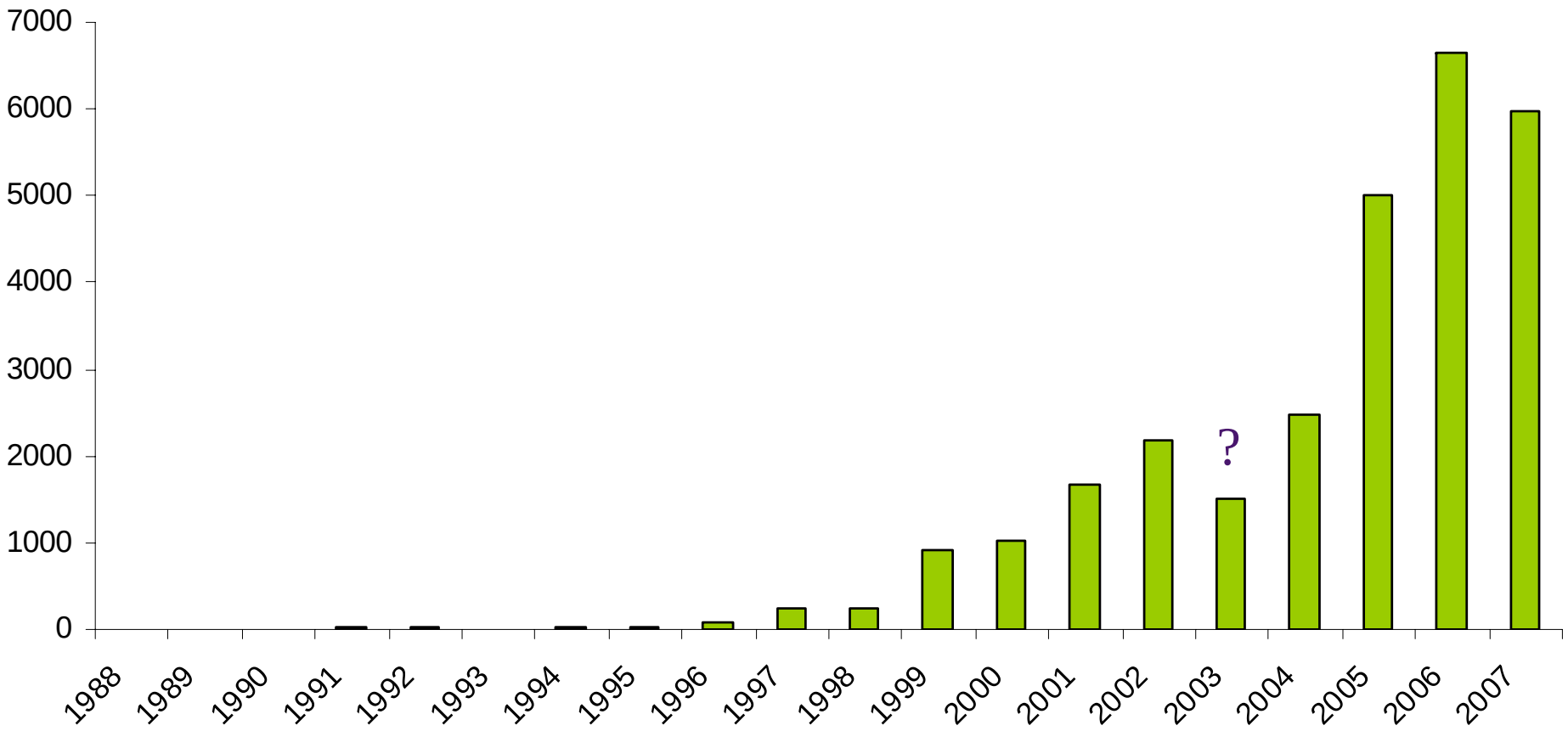
- VR Engineering Report
- Production-quality IDS/IPS Signature, VA Probe, & PoC exploits

Assurent VR processes

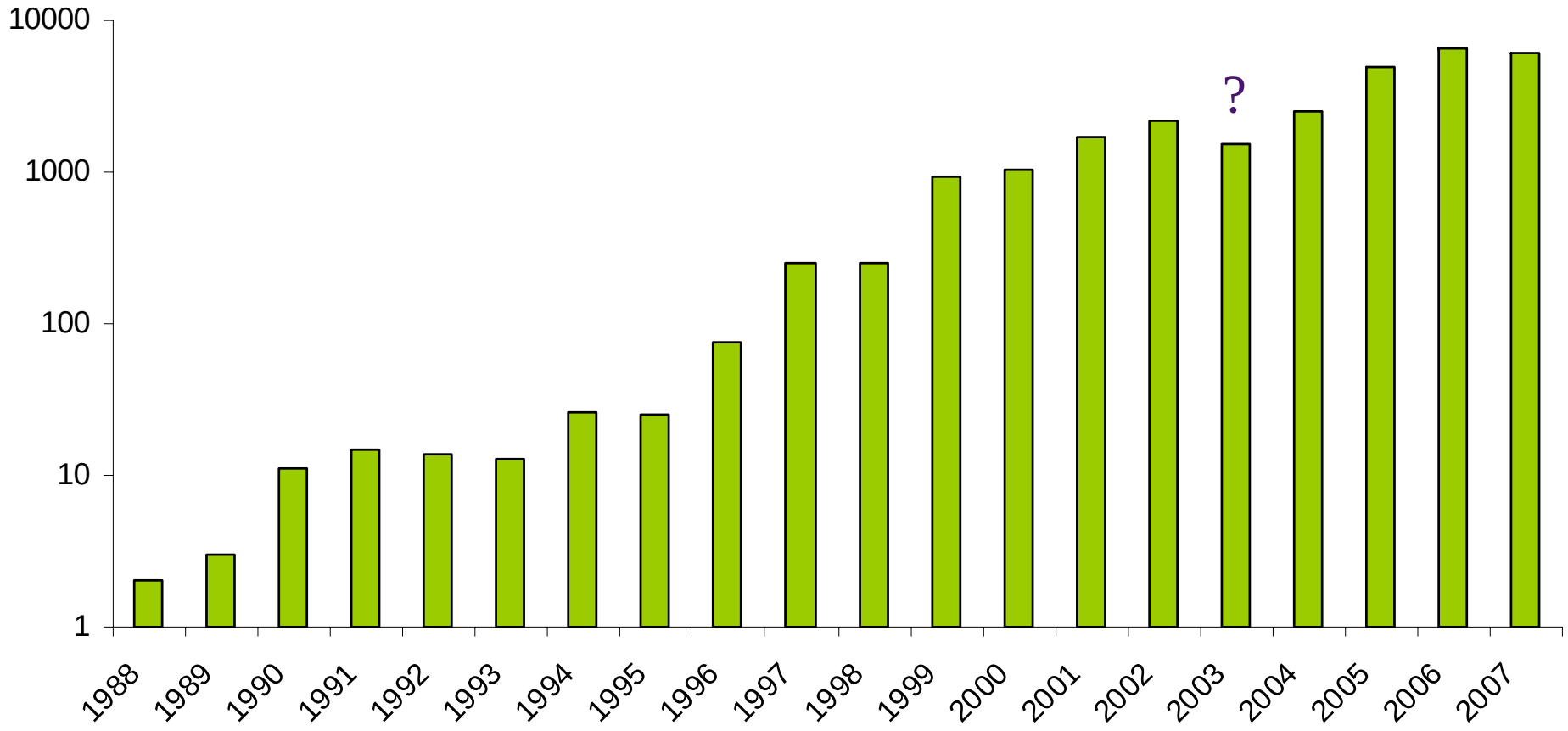


What do we see?

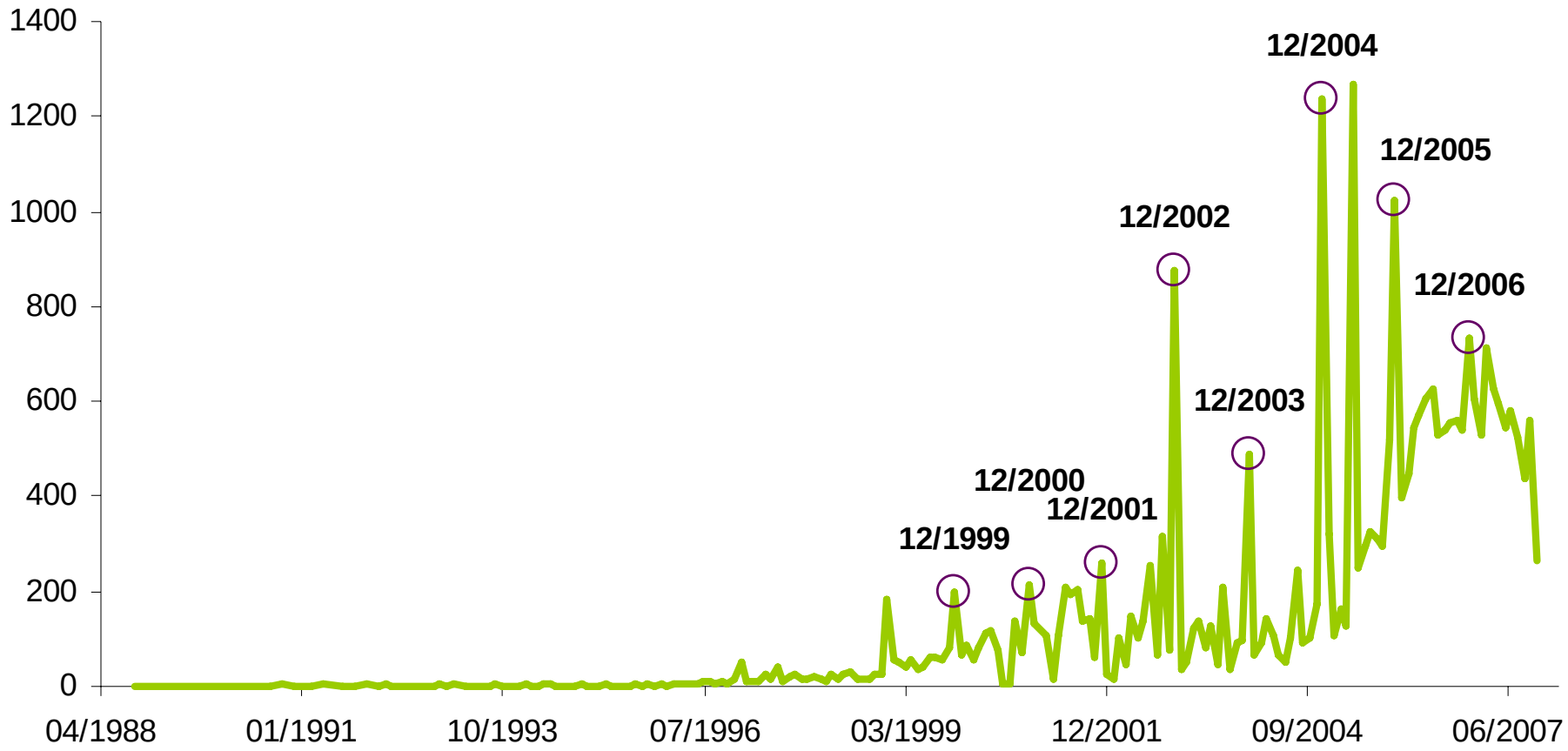
High-level summary statistics



High-level summary statistics (logarithmic)



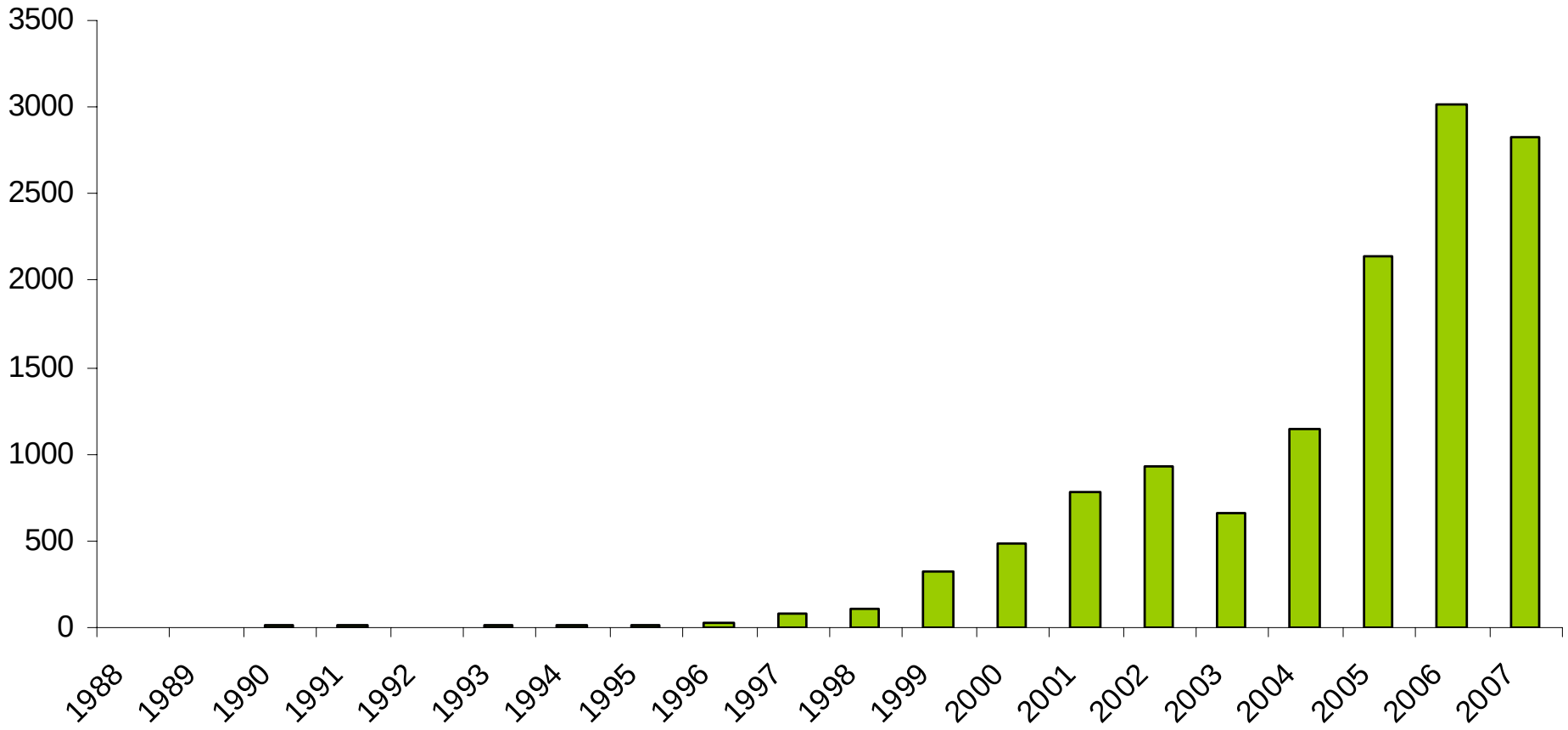
End of year spikes



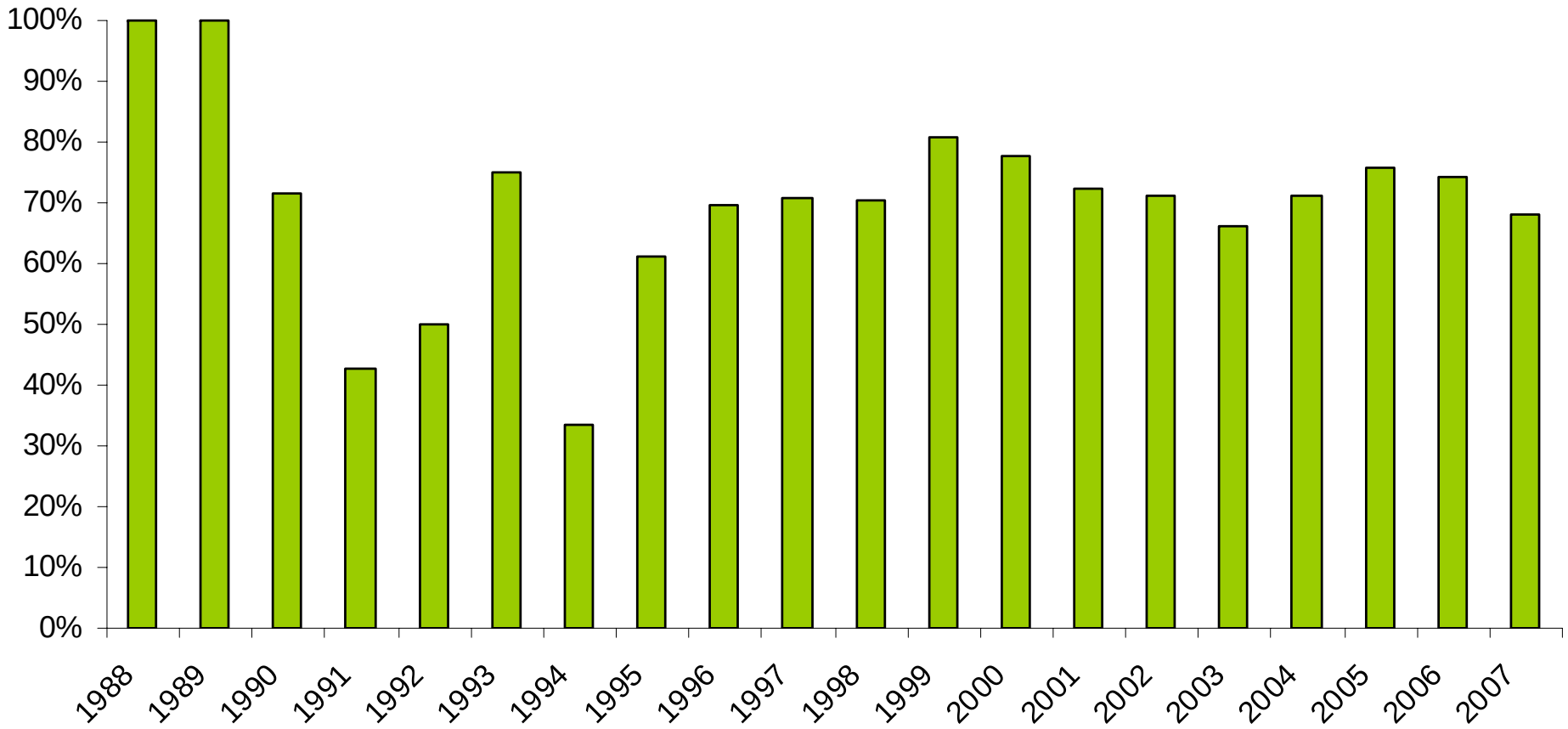
High-level statistics – Summary

- Can we explain the end-of-year spikes?
  - There are mid-year spikes too

Products per Year



New products per Year

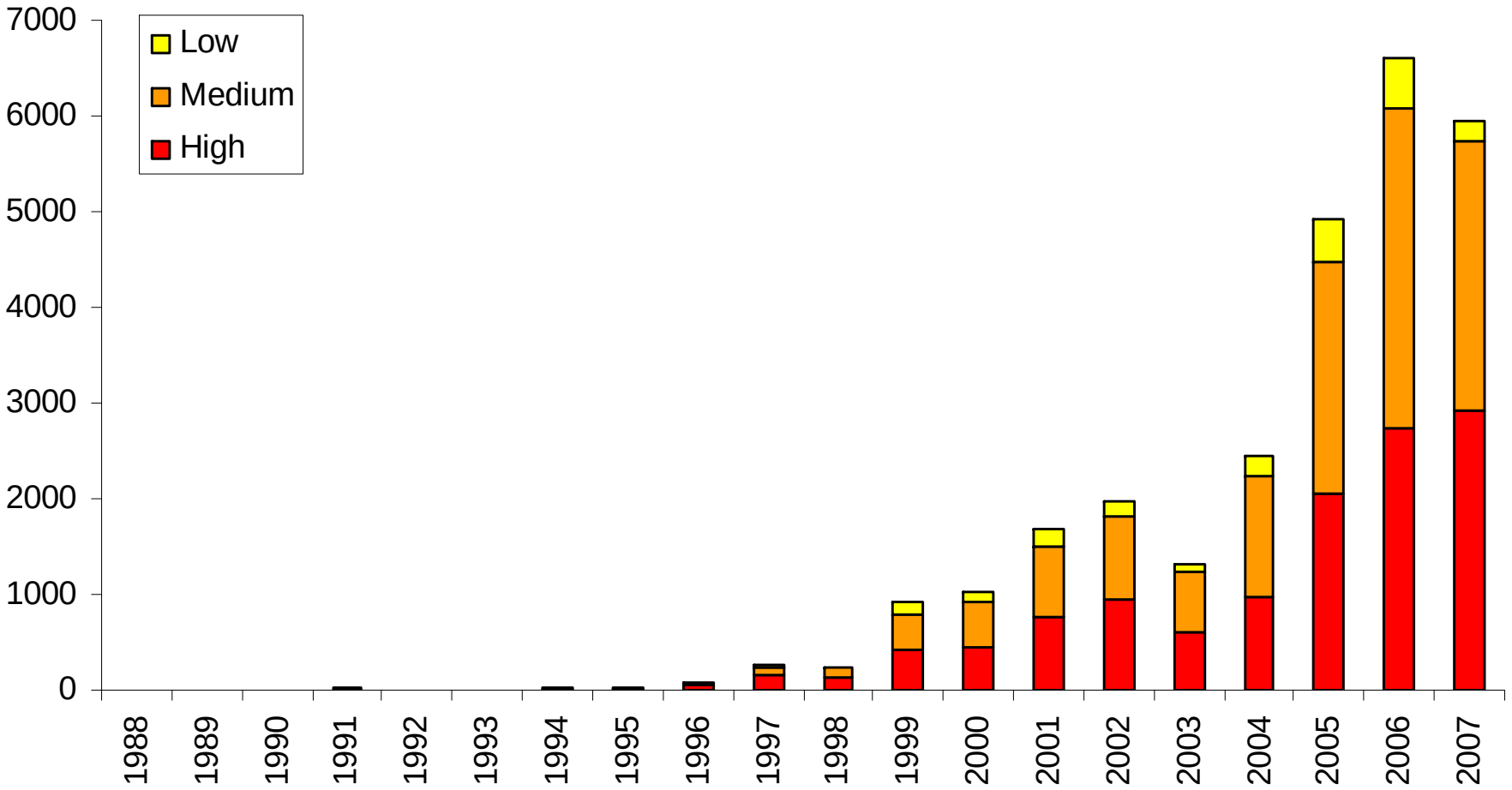


New products per Year

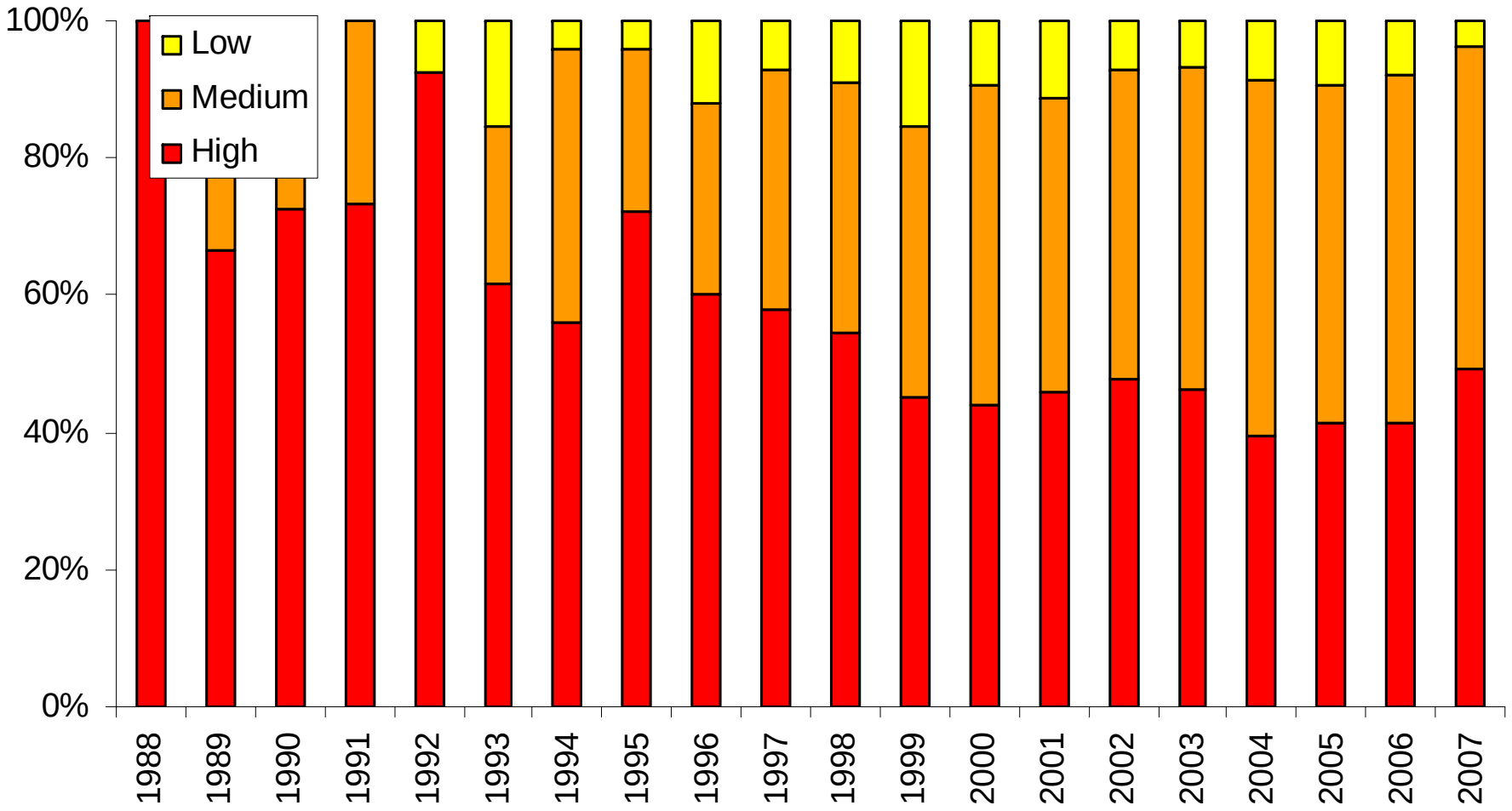
- Most of the effort goes into new vulnerabilities
- What about older software revisions?
- Is the market testing my software?

Data on vulnerabilities

Bad news sells

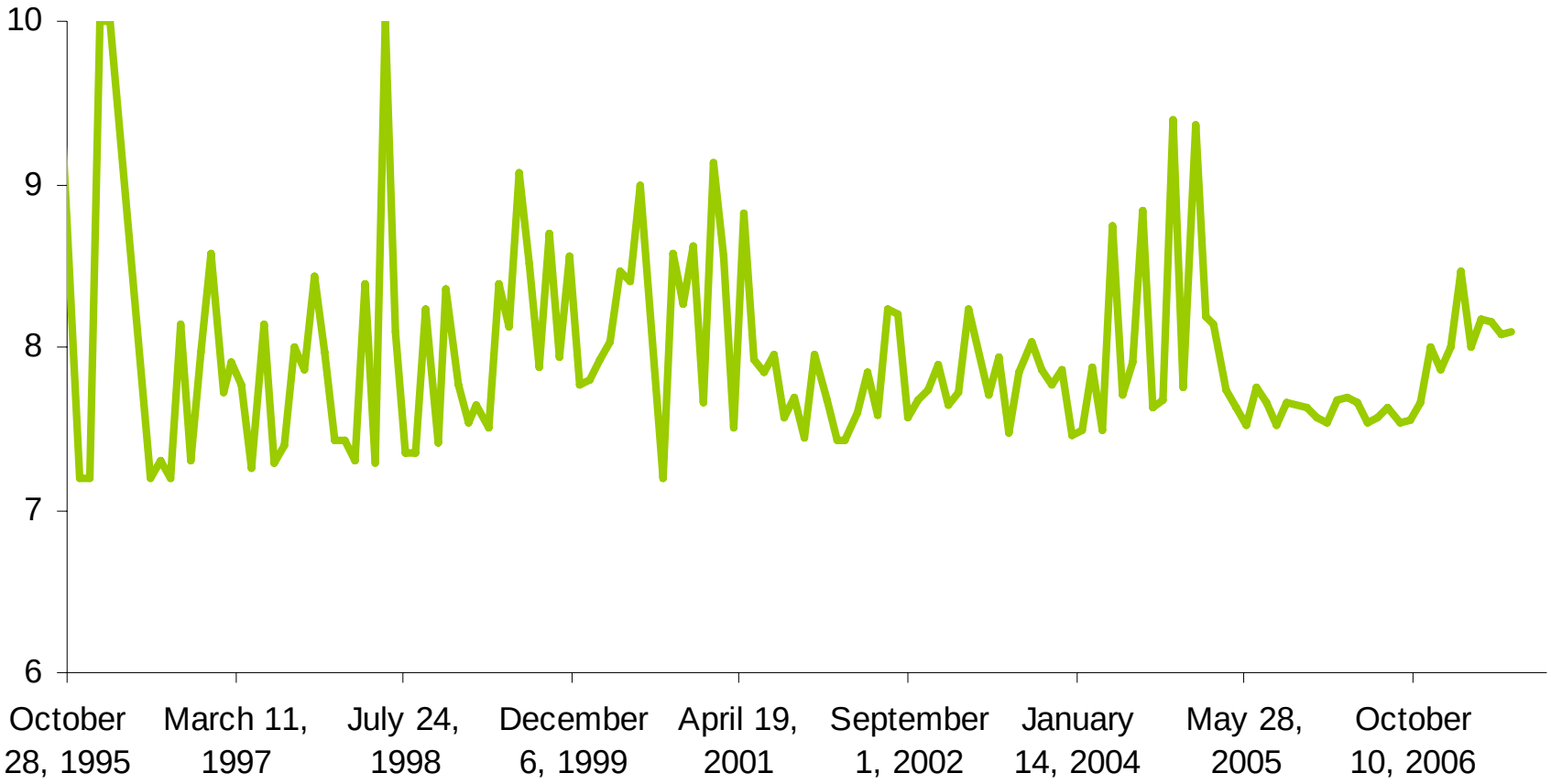


Are we getting better at impact reduction?



TELUS®

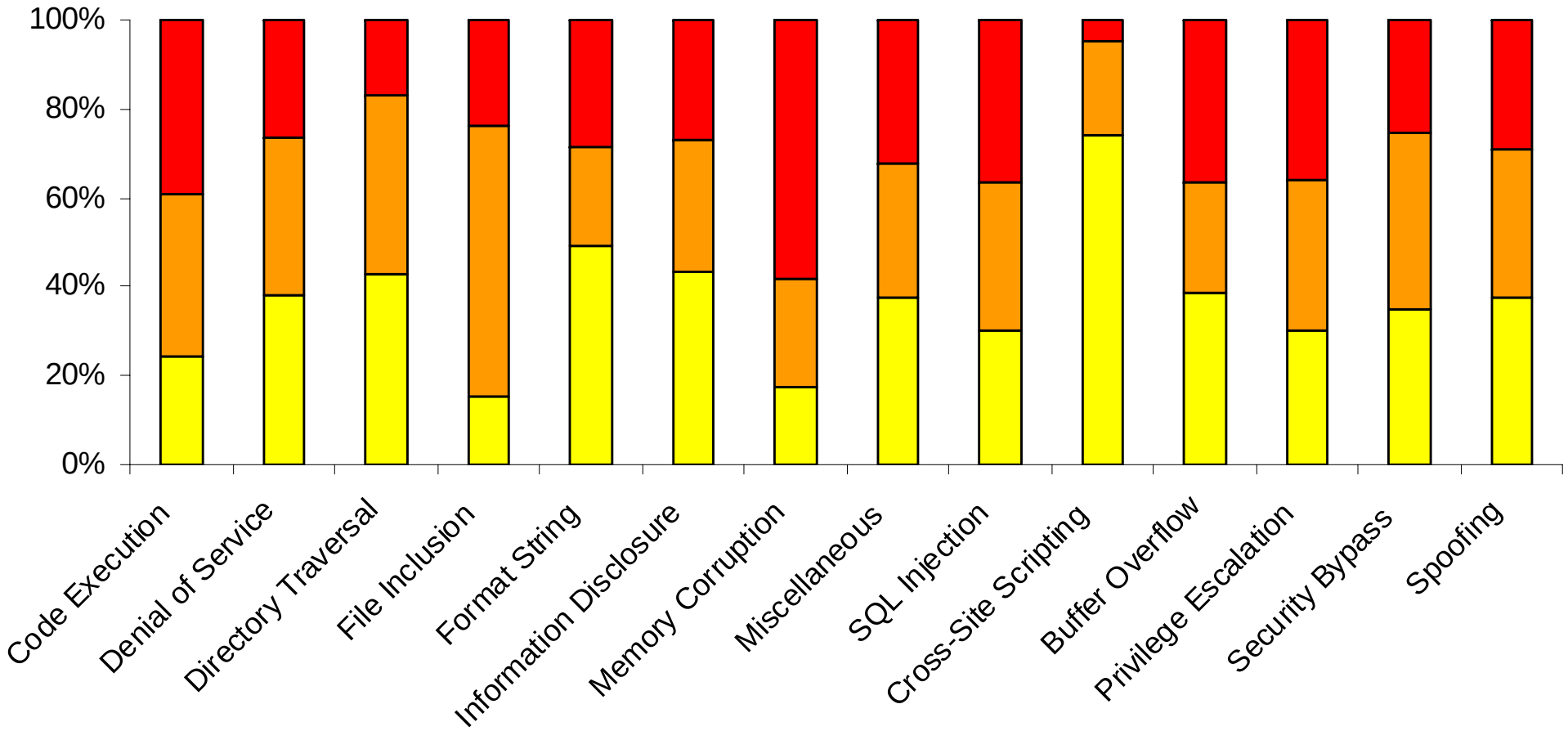
Is the bad getting worse?



It’s not getting worse

- …it’s relatively stable
- … and appears to be getting a little better
- … not all is reported

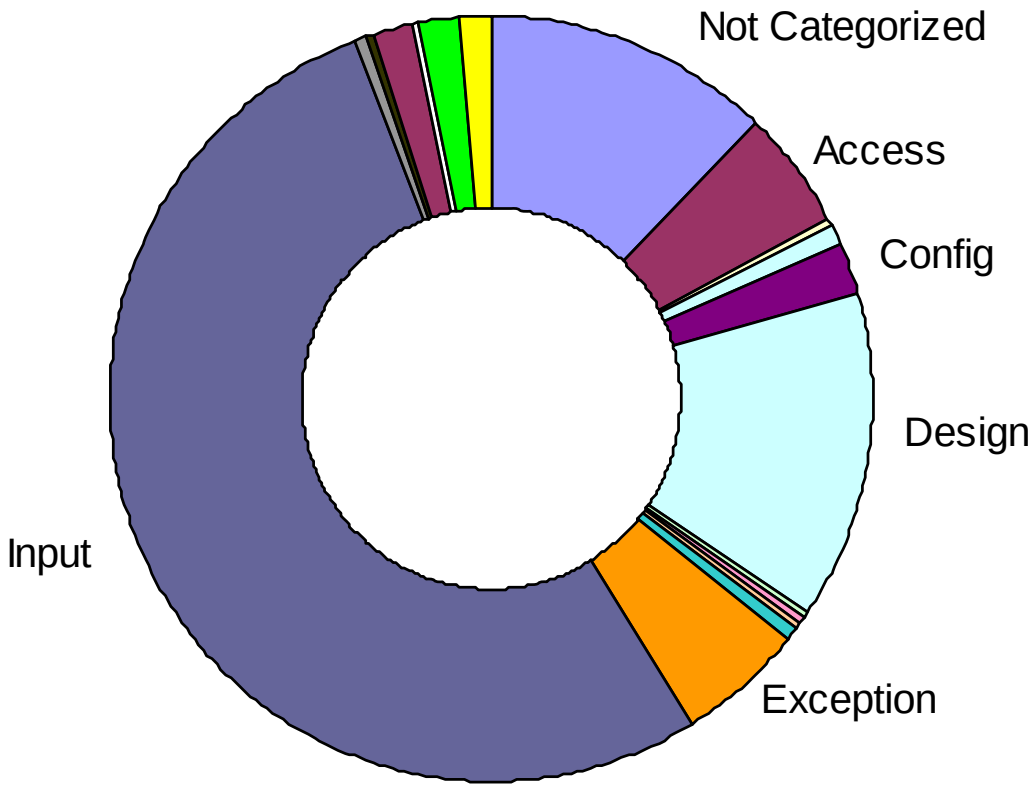
What's the worst vulnerability type?



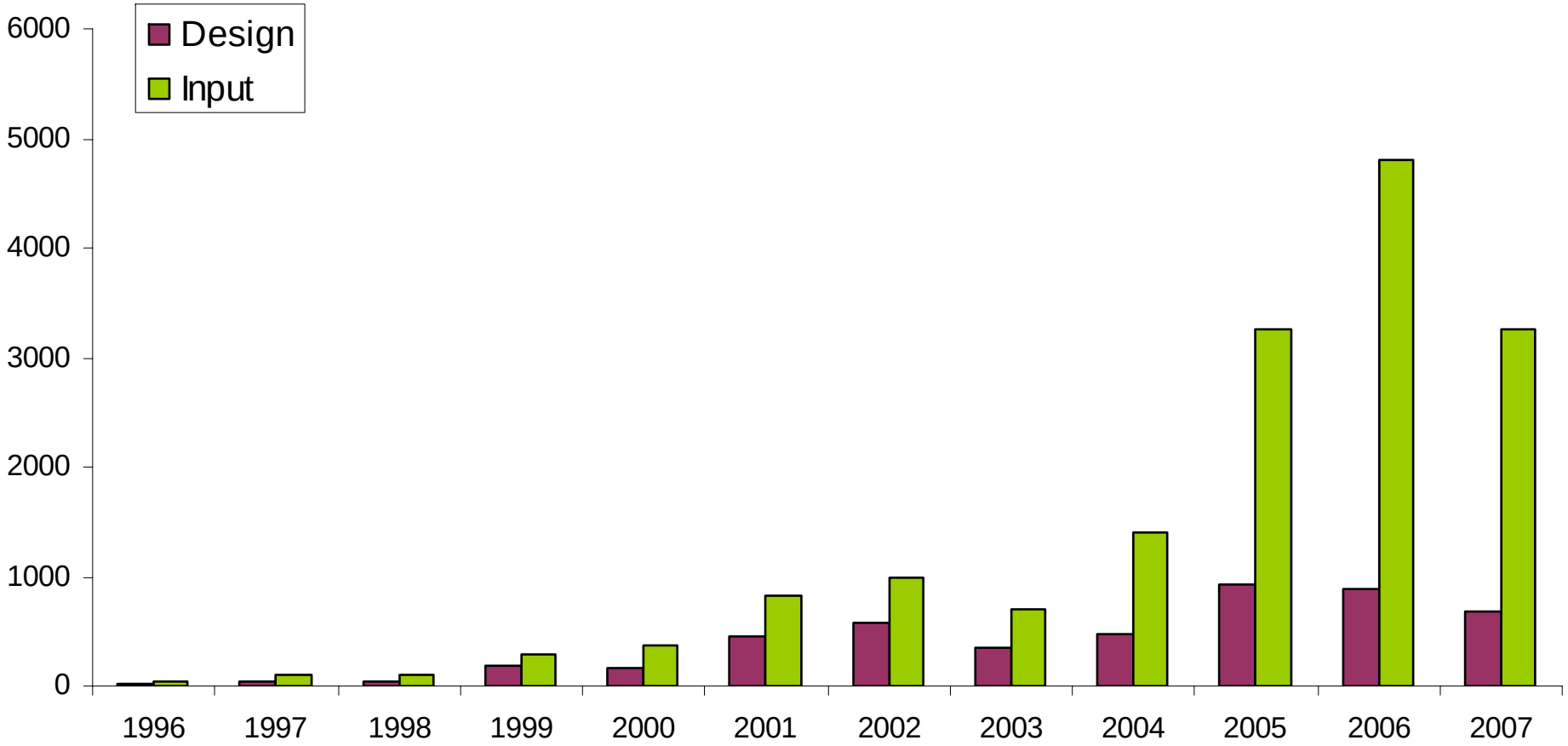
Data on vulnerability types - Summary

- Buffer overflows/Non-byte-code continue to be the most common vulnerability type
- Buffer overflows also have the highest rate of criticality
- Web-application vulnerabilities are prevalent
  - Lower proportion of reported vulnerabilities
  - XSS isn't that bad

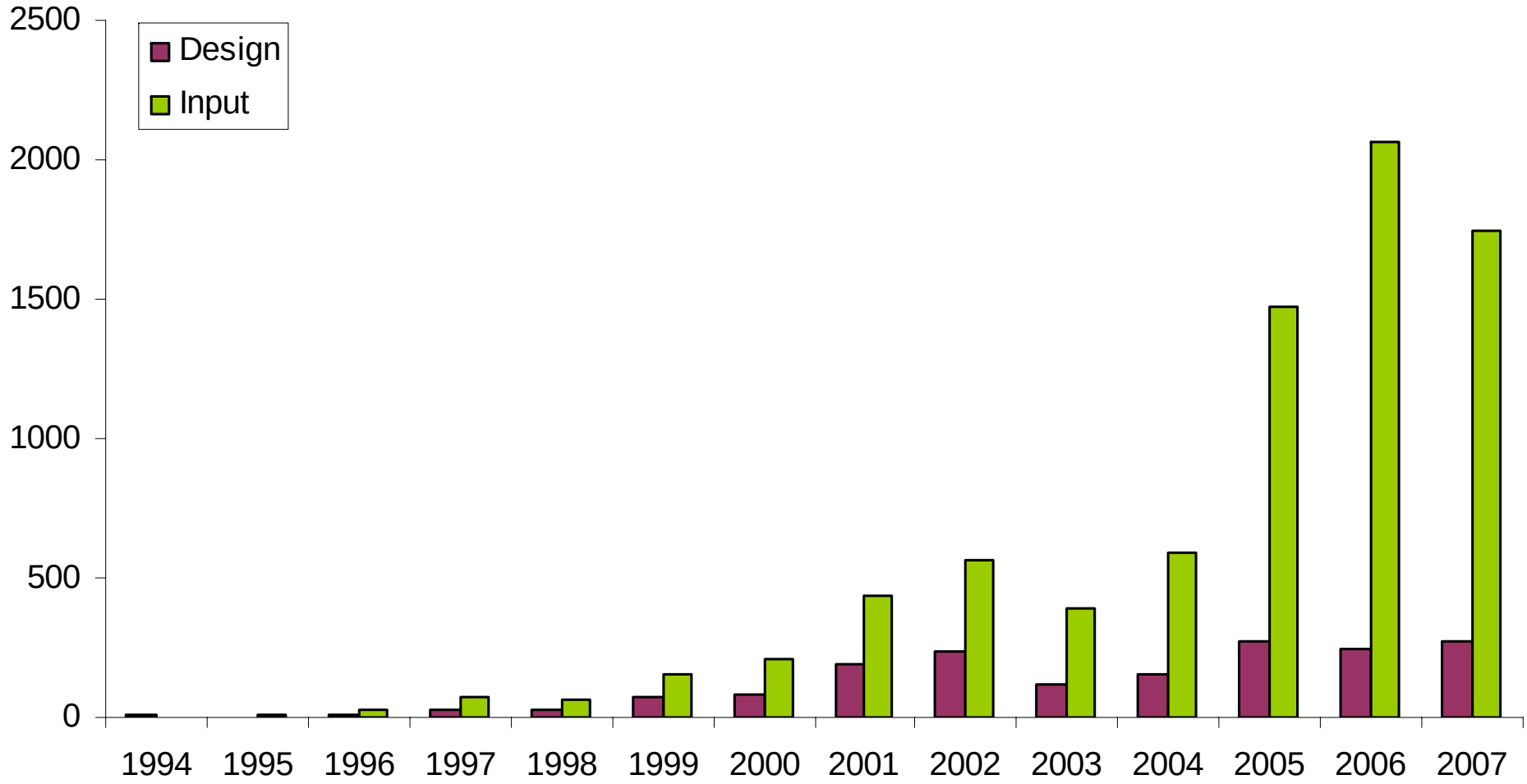
Distribution of Vulnerabilities



Design vs. Implementation



Design vs. Implementation (High)



Design vs. Implementation

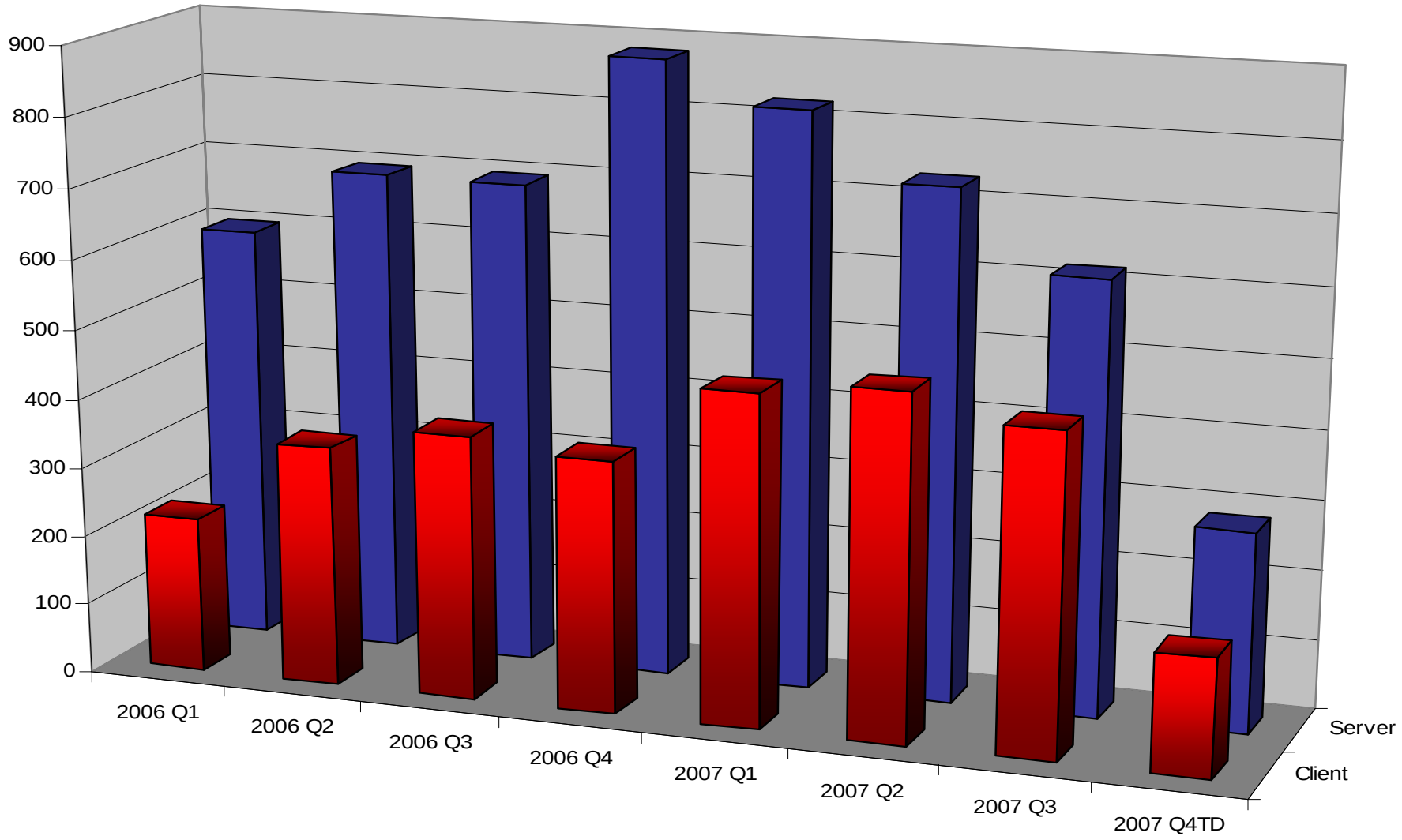
- Design issues will overtake Implementation around Sept 2197
- Remediation costs are much higher

Design vs. Implementation

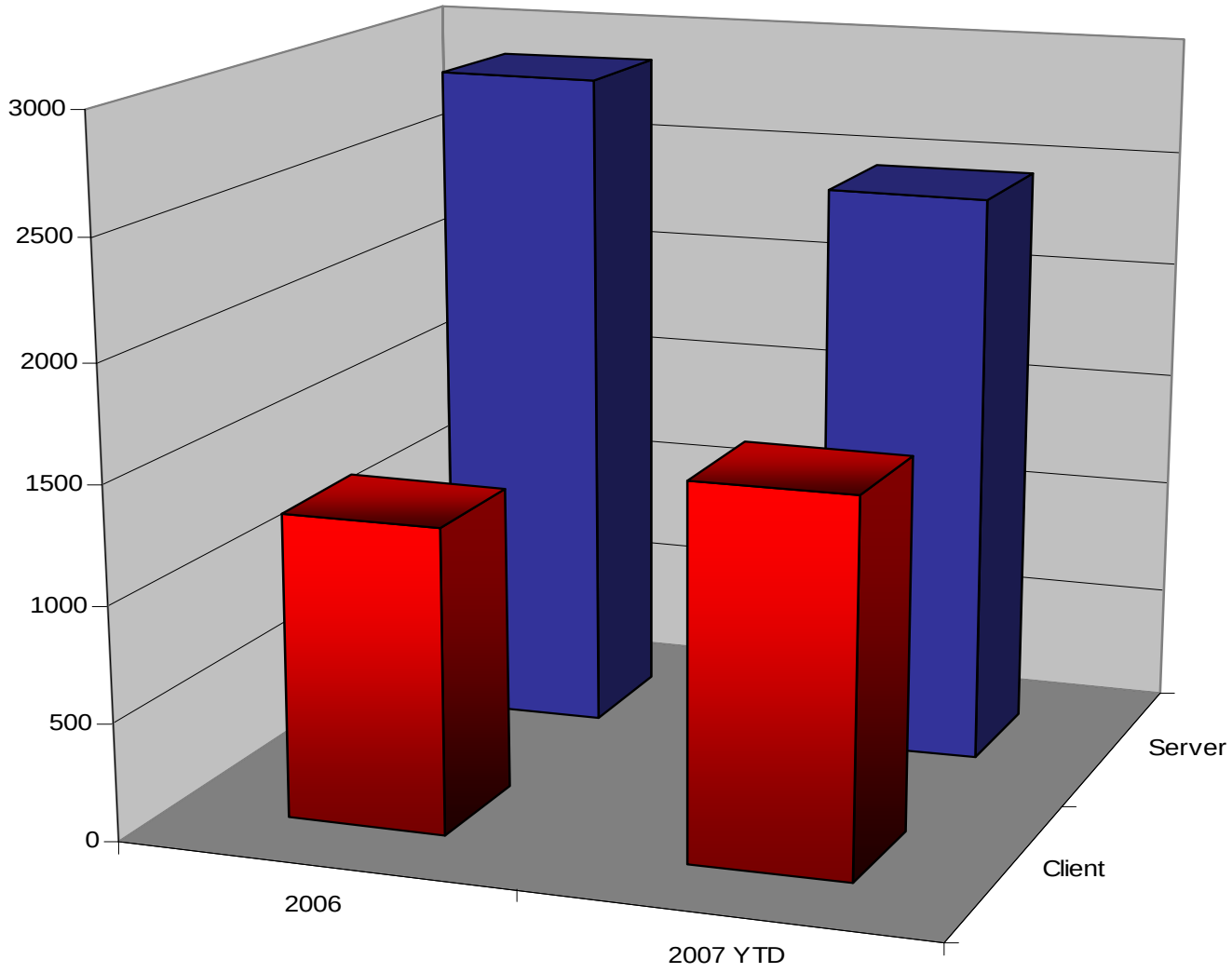
- Stack Smashing/Heap still has the best ROI

Where do I want to invest by defensive dollar

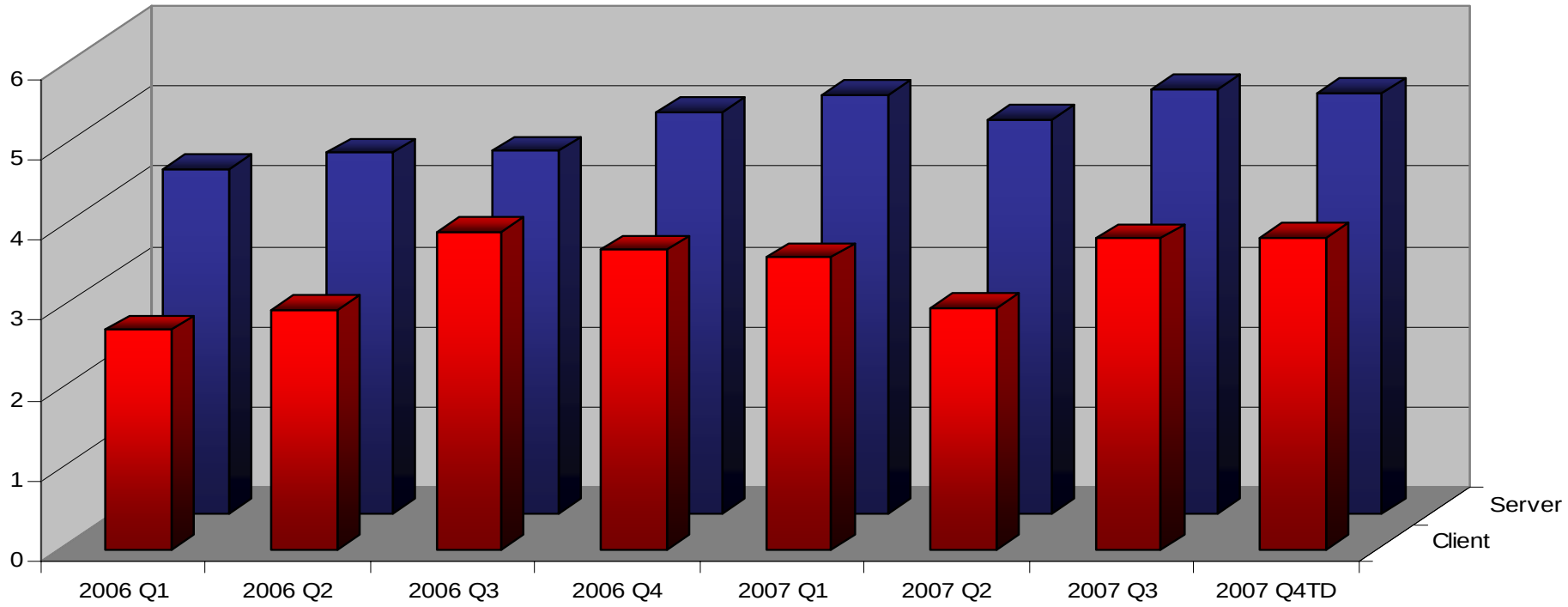
Client vs. Server Vulnerabilities by Quarter



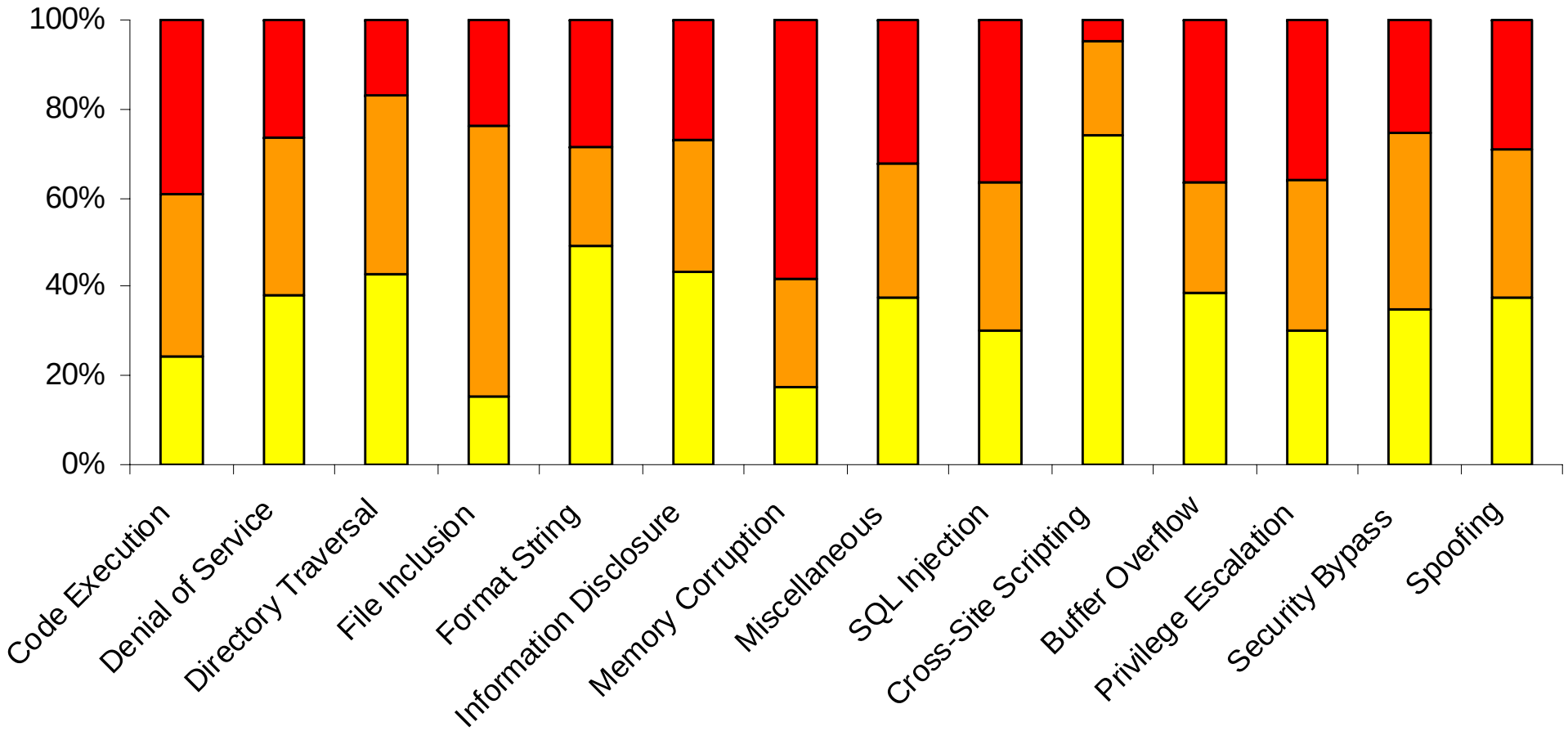
Client vs. Server Vulnerabilities - 2006 vs. 2007



Mean Severity (CVA), Client vs. Server, by Quarter



What's the worst vulnerability type? (revisited)

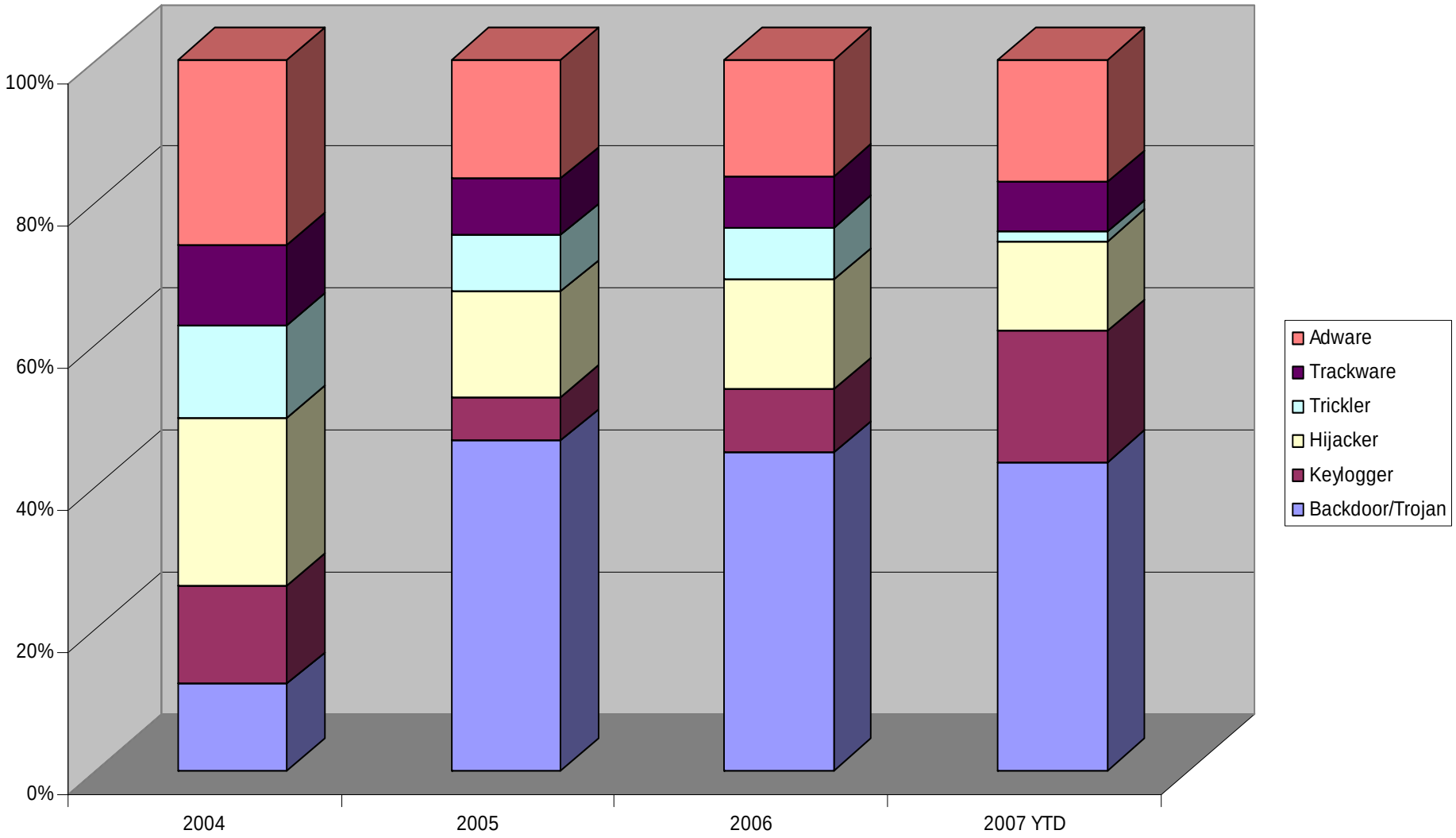


Investing the defensive dollar – Summary

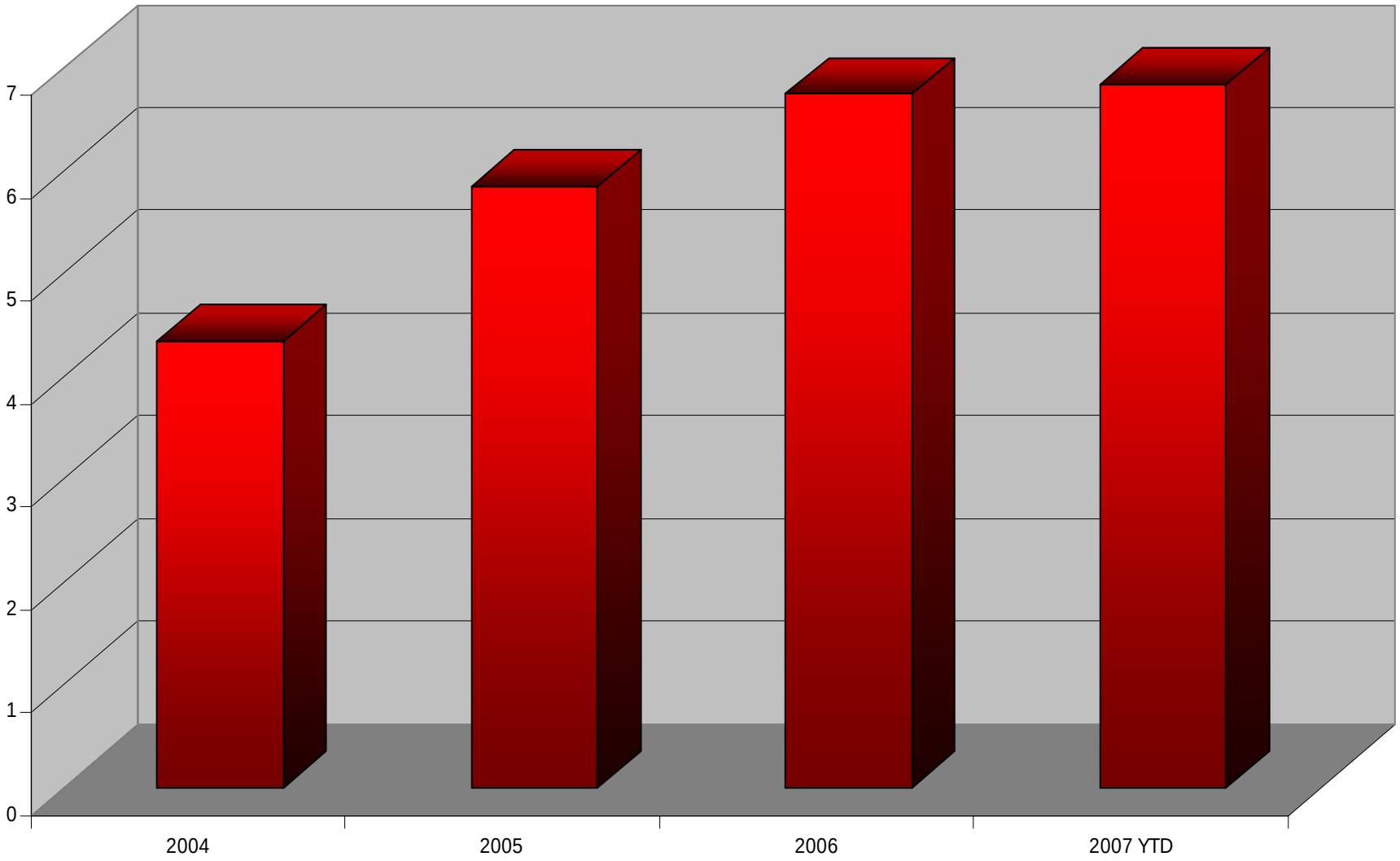
- Server vulnerabilities still outnumber Client vulns
- Client vulnerabilities are climbing
- Server vulnerabilities are rising faster
- Upward severity trend is quite consistent quarter by quarter
- Safe languages and secure development practices

Spyware

High-Risk Spyware by Type, 2004 - Present



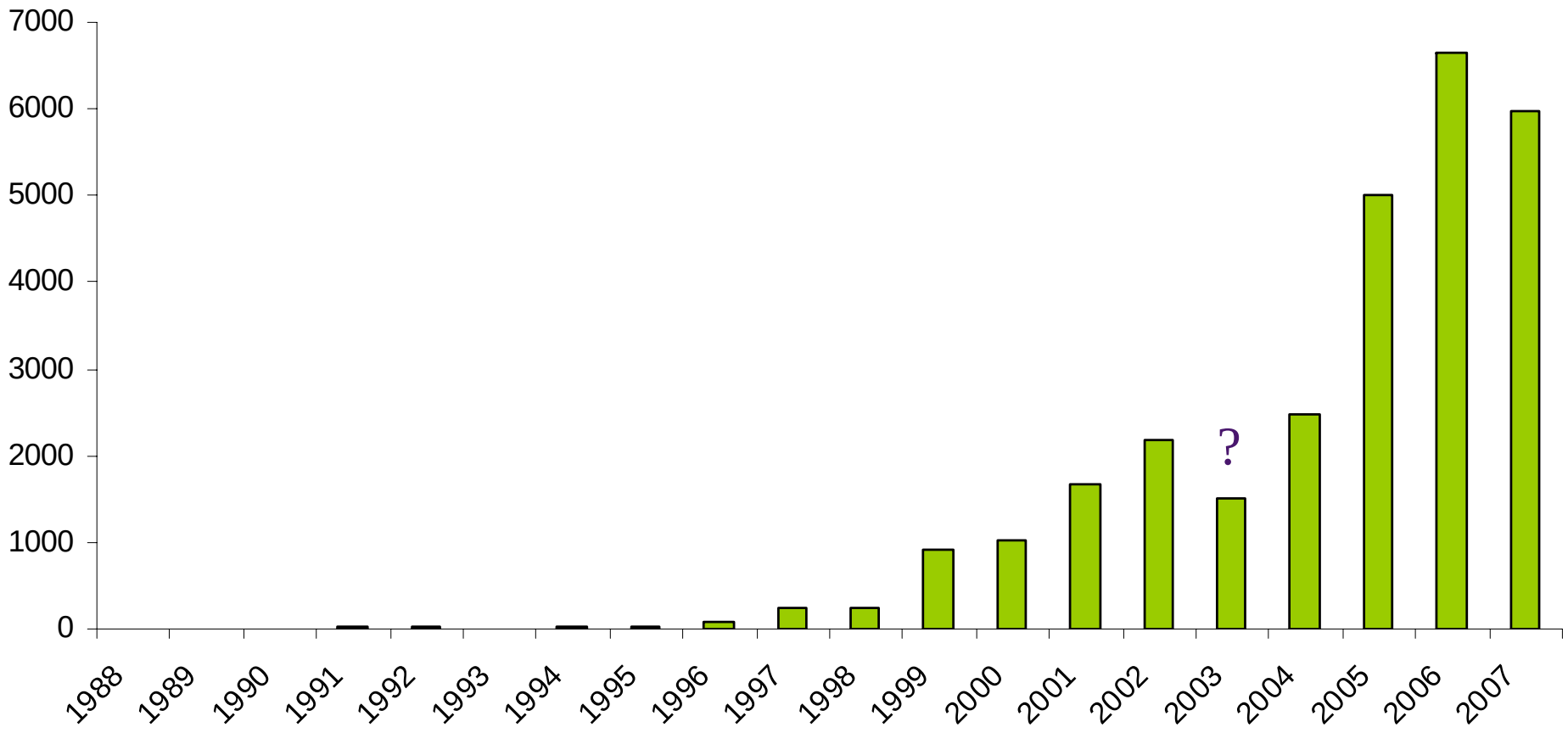
High-Risk Spyware - Average Severity



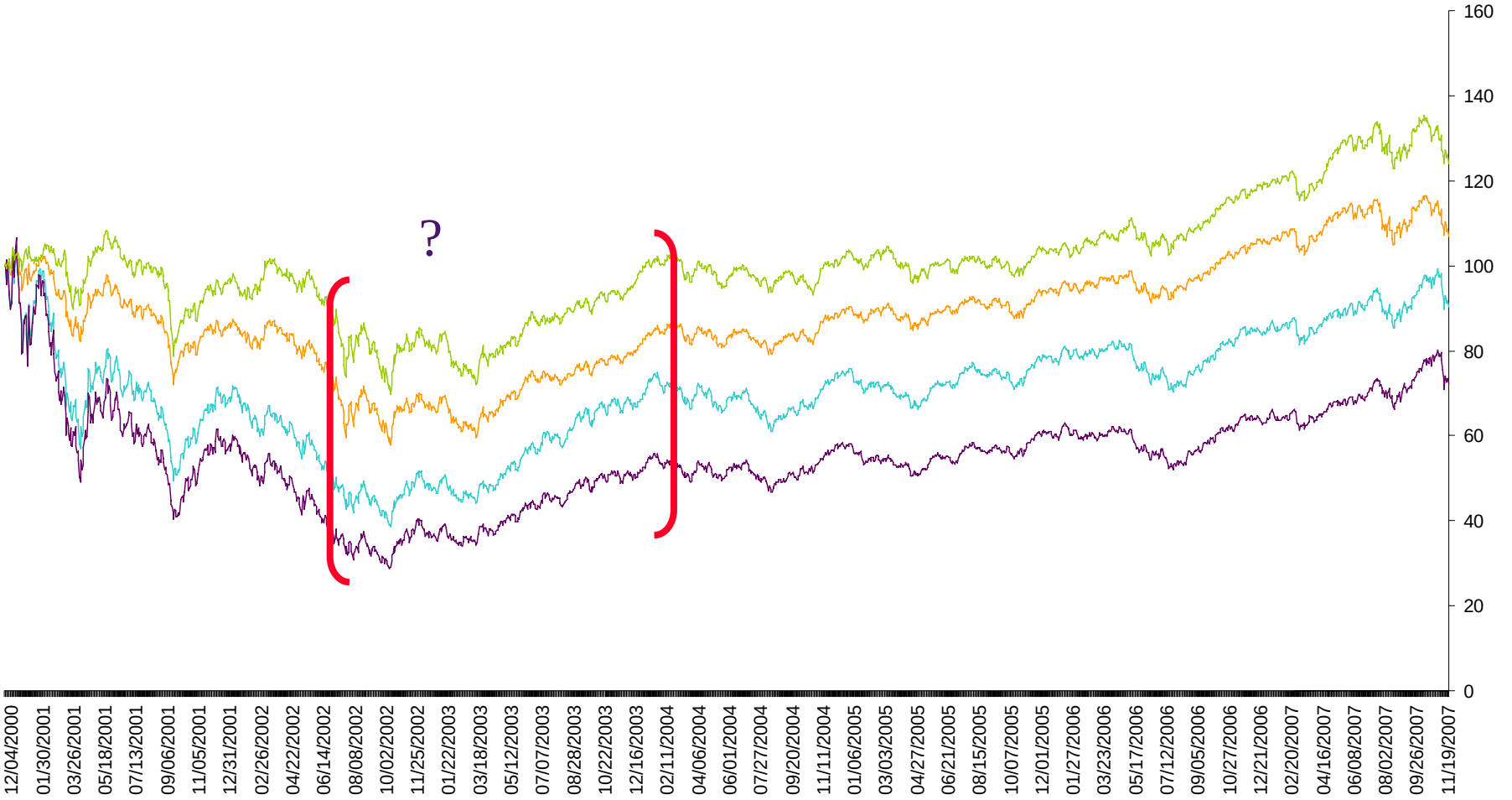
Spyware - Summary

- Backdoors & Keyloggers majority of High-risk spyware
- Low-severity spyware is dying off
- Average risk of spyware population is trending upwards

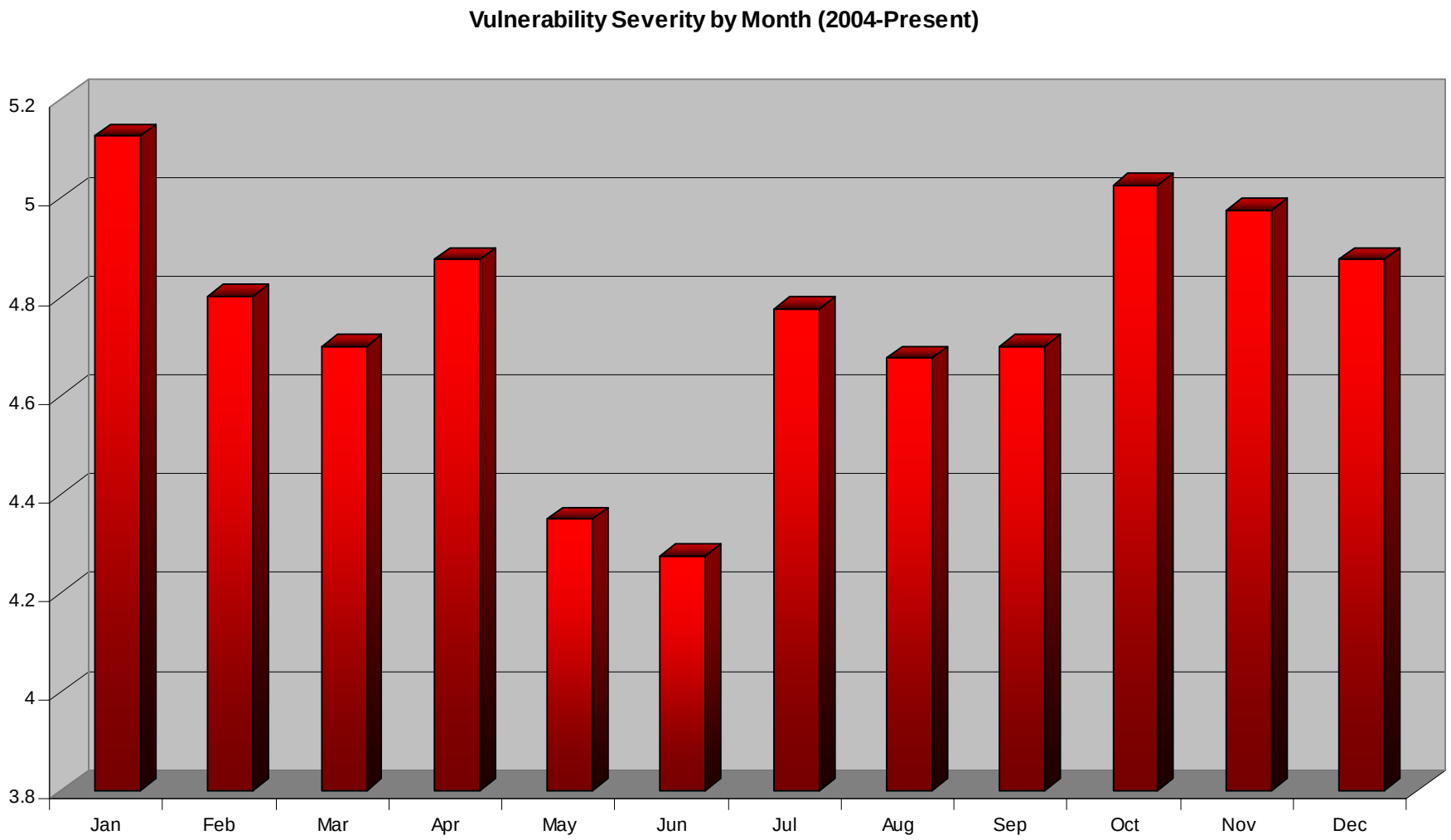
So what happened in 2003?



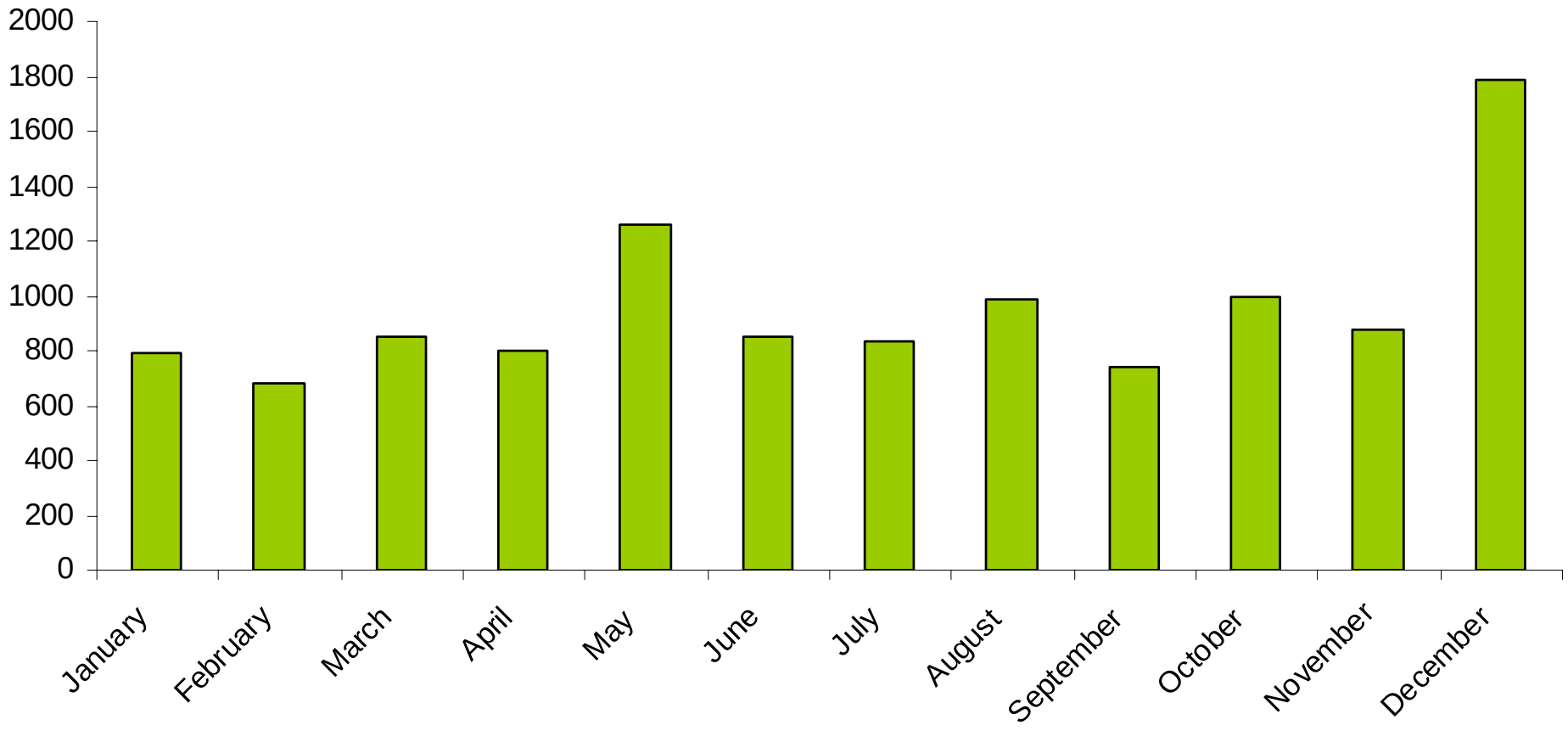
So what happened in 2003?



When should I take vacation?



When should I take vacation?



When should I take my vacation?

- Security people like their summers off?
- Students write their exams in May & June?
- Everyone spends more time indoors in the (Northern hemisphere) winter months?

Conclusions

- We aren't getting (materially) better at minimizing impact
  - Failure to implement key principles such as:
    - Complete Mediation
    - Least Privilege
- Vulnerability Research is inherently biased and only as good the *-hats powering it
  - For-Pay research increases the bias
  - We need to invest in greater automation
  - Further standardization of information collection
- We need to invest more effort in secure coding and design

Conclusions

- Custom software is unreported
  - Hard to extrapolate
  - Under our control (good thing™)
- Historical vulnerability data could be useful for Cost of Ownership arguments

Conclusions

- Observations
  - Is XML the best way to share vuln data?
  - CPE is a library, not a taxonomy
  - CWE x-ref is a good thing
  - MySQL plus a Ruby dev > MSSQL and a VBA dev
  - Queries that take 5 minutes to run are cool…
  - The general state of vuln data collection does lend itself to structured/programmatic analysis

TELUS Security Solutions

Questions & Comments

TELUS
the future is friendly®