Mini-Metricon 5.5

Reforming the Vulnerability Disclosure Process (part 1)

Preliminary Work

Idaho National Laboratory

University of Idaho
Idaho Falls

How long should the vendor be given to provide a patch (**and** who should make the decision**)**

Miles McQueen

Idaho National Laboratory and University of Idaho

Jason Wright, Lawrence Wellman

Idaho National Laboratory

February, 2011

San Francisco

How long should vendors be given?

Security firm positions…

Idaho National Laboratory

University of Idaho Idaho Falls

❖ "…**Rapid7**, where HD Moore is Chief Security Officer and Chief Architect of Metasploit, recently revamped their disclosure policy. In short, they will hold a vulnerability for **15 days** after contacting the vendor, before sending it to CERT, who will give the vendor another **45 days** to address the issue…." ---The Tech Herald, August 2010

❖ "…the Zero Day Initiative (**ZDI**), part of Hewlett-Packard / TippingPoint, has announced that, with immediate effect, it will limit the period for developing security updates to **six months**. However, the ZDI says that it will grant extensions to this deadline in special cases…." --- The H Security, August 2010

❖ "Serious bugs should be fixed within a reasonable timescale. Whilst every bug is unique, we would suggest that **60 days** is a reasonable upper bound for a genuinely critical issue in widely deployed software. This time scale is only meant to apply to critical issues. " --Chris Evans etal, **Google** security Team, July 2010

❖ "All vulnerabilities reported to the CERT/CC will be disclosed to the public **45 days** after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors. Extenuating circumstances, " --**CERT/CC** 2008

❖ "The best way is to quietly disclose the problem to the vendor and then allow the vendor **30 days** to fix the problem. Then go public," --**Phil Zimmermann** 2005

Why those disclosure times

Noble intentions?

Idaho National Laboratory

University of Idaho Idaho Falls

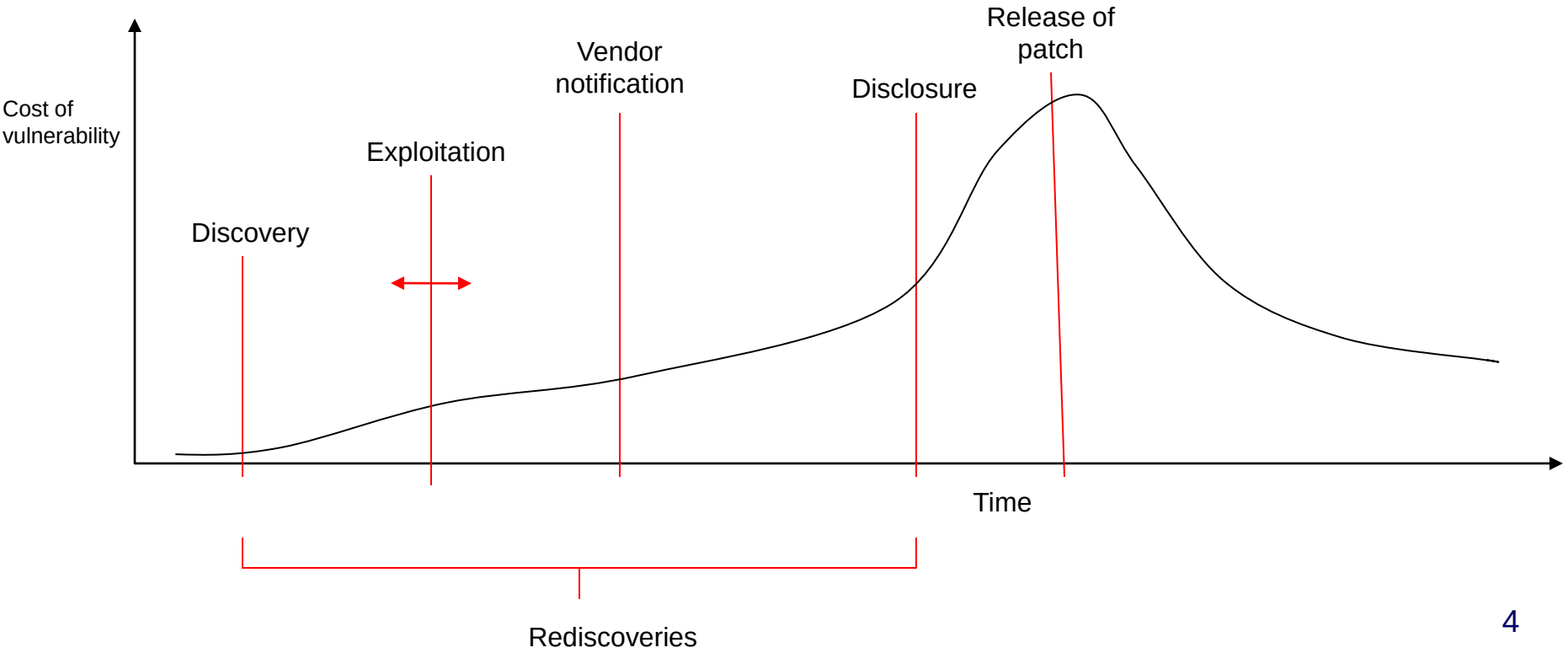
❖ "For every day a vulnerability goes unpatched, end users are susceptible," Portnoy said in an interview. "Vendors are being a little bit irresponsible by not patching them." **--ZDI (CRN), Aug 2010**

❖ "…will result in smaller windows of opportunity for blackhats to abuse vulnerabilities. In our opinion, this small tweak to the rules of engagement will result in greater overall safety for users of the Internet." **–Google, Sept 2010**

Across businesses

Can't dependably and verifiably know discovery date.
Can't dependably and verifiably know rediscoveries.
Can't dependably and verifiably know all exploitation dates.
Can't dependably and verifiably know loses from vulnerabilities, nor costs to fix.

May dependably and verifiably know vendor notification date.
May dependably and verifiably know date patch is released.
May dependably and verifiably know disclosure date.



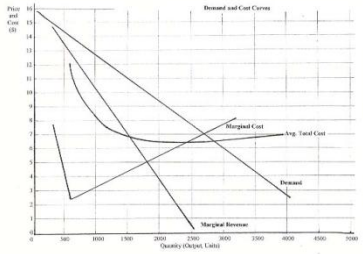
Transparency

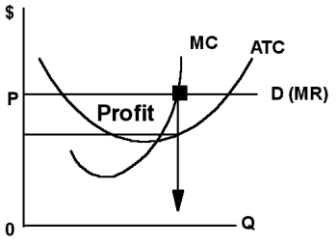
Dependable and verifiable vulnerability information

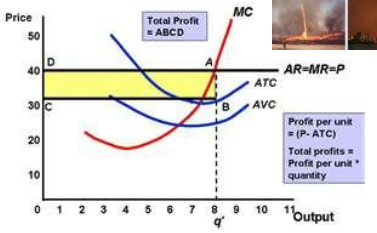
Idaho National Laboratory

University of Idaho Idaho Falls

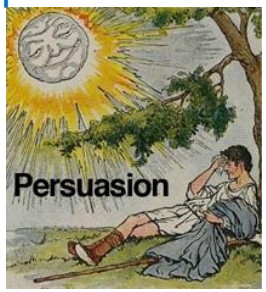
- Vendors should
  - Provide timely, accurate, and easily accessible vulnerability data by major product release.
  - Date reported to them
  - Who reported it to them
  - Current disposition
  - Anticipated patch availability date
  - Actual patch availability date
  - Space for vulnerability discoverers comments
  - …







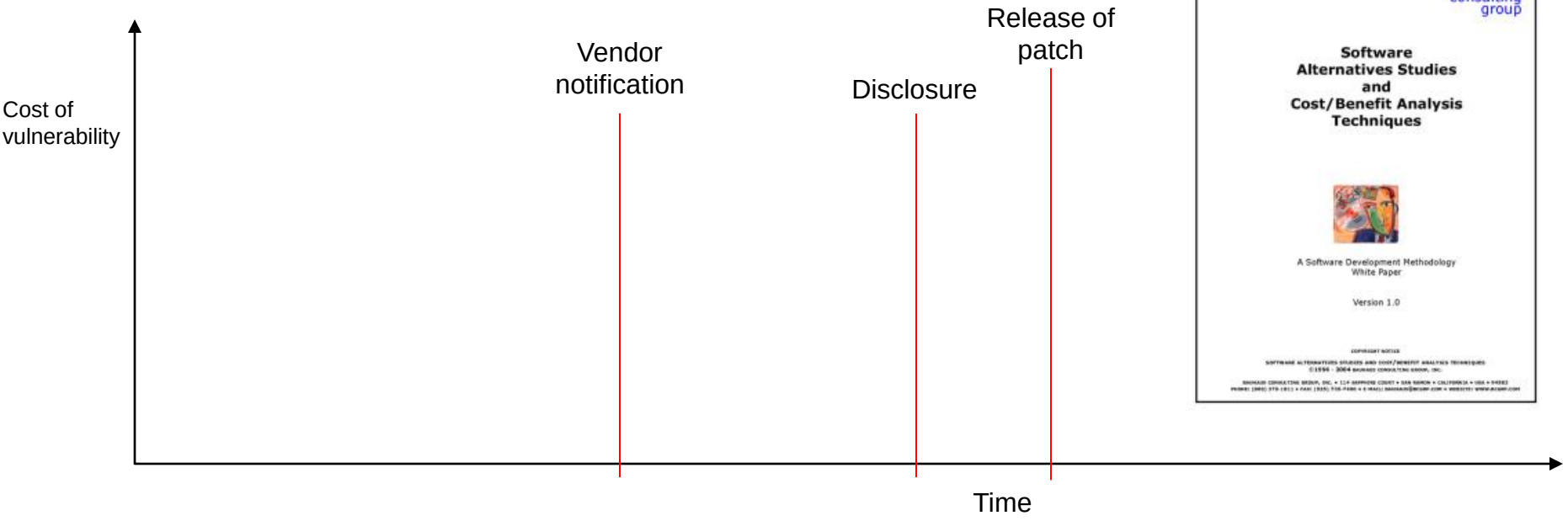
- Security researchers should
  - Never publicly provide full disclosure
  - Keep track of vendor's response to their reported vulnerability (keep them honest) and comment if inaccurate
  - …



- End users should
  - Track vendor performance
  - Use vulnerability metrics (to aid 'allowed use'/purchasing decisions)
  - Apply pressure…

End user perspective?

- Reduce time between disclosure and release of patch.
  - C'mon security researcher, cut it out
- Reduce time between vendor notification and release of patch.
  - Hurry up vendor, provide a patch
- Fewer software vulnerabilities (iffy proposition…).
  - C'mon vendor, produce less flawed software!

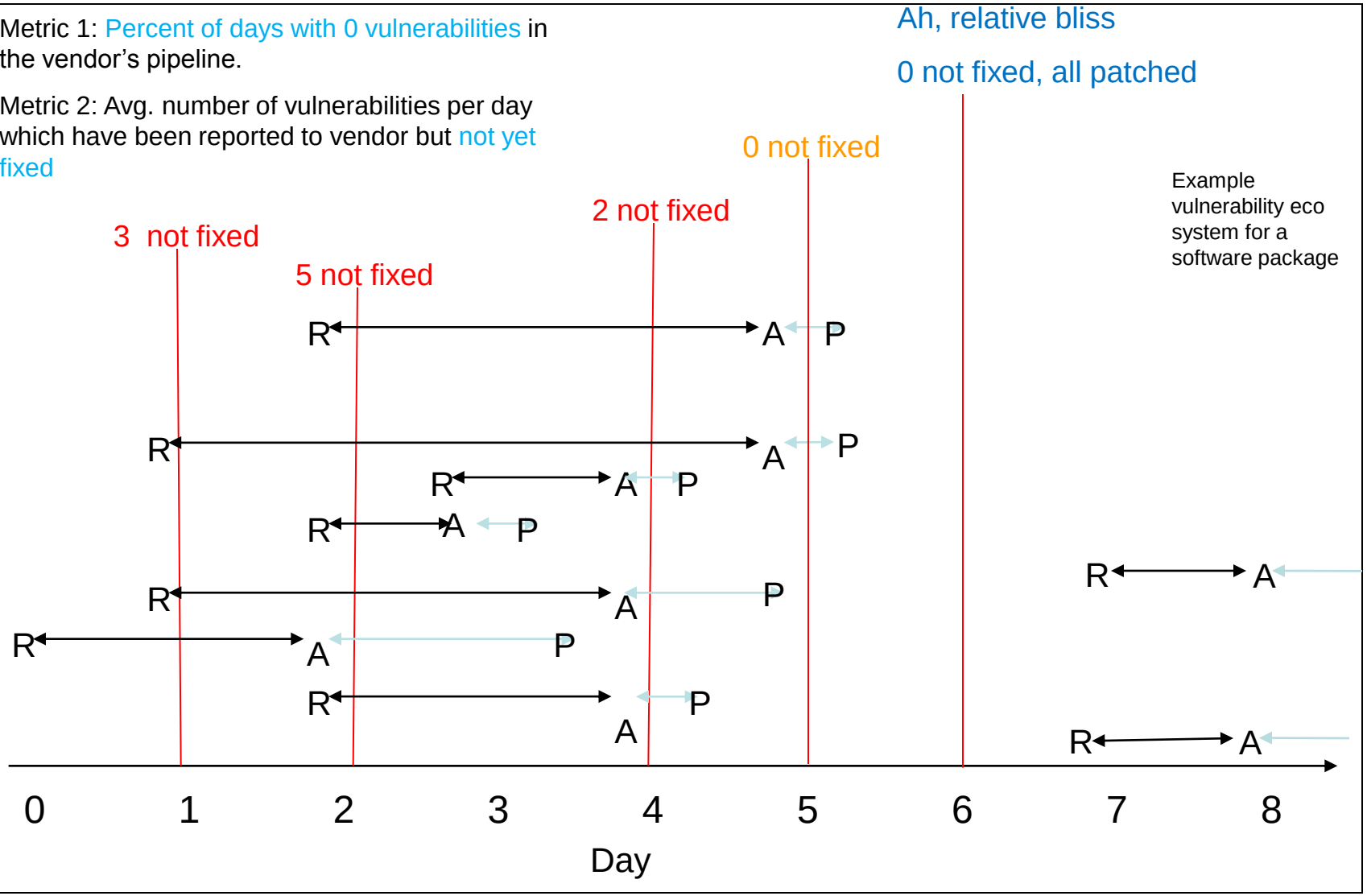


Two proposed metrics

Intuition

Metric 1: Percent of days with 0 vulnerabilities in the vendor's pipeline.

Metric 2: Avg. number of vulnerabilities per day which have been reported to vendor but not yet fixed



Conclusion

Embrace the diversity of end users, vendors, and their products

Idaho National Laboratory

University of Idaho
Idaho Falls

- Acknowledge one size does NOT fit all
  - Every product is different.
  - Every end user has different costs and benefits.
  - Every vendor has different costs and benefits.

- Perfect information and intentions do not, and will not, exist
  - No ORACLE or wise man who knows everything.
  - Few, if any, saints involved in the process, including security researchers.

- For individual end users and vendors to make rational business decisions, dependable and verifiable information must be freely and easily available.
  - Must work with what is realistic to know (opinions can vary)
  - Need to provide benefit to vulnerability researchers
  - Useful metrics need to be developed by the community

We have completed today's talk

Idaho National Laboratory

University of Idaho
Idaho Falls

There is much more to discuss

I am interested in your thoughts…

So please feel free to contact me

In conjunction with the International Symposium on Resilient Control Systems

August 11th, 2011

Boise, Idaho

https://secureweb.inl.gov/ISRCS2011/ESP.aspx

Contact Information

Miles McQueen	amm@if.uidaho.edu or Miles.McQueen@inl.gov	(208)-526-5872 (208)-206-5005

Note

Idaho National Laboratory

University of Idaho
Idaho Falls

These slides have been edited for general posting and represent only a portion of the slides actually used at Mini-Metricon 5.5

I am interested in your thoughts…
So please feel free to contact me