Responsible Disclosure?

Michael Kemp
Senior Security Consultant
Computer Sciences Corporation

Who am I?

- Over five years experience in IT security
- Have been a consultant, researcher and technical specialist – know the vulnerability disclosure process from both sides
- Have worked with some of the best security researchers in the world (and some of the laziest developers – not, it should be mentioned in the same place)
- Do not have a huge number of published vulnerabilities for many reasons…

Disclaimer

- It should be noted that any ideas, views or opinions expressed in this presentation or supporting materials, are in to way indicative, reflective or representative of the views, opinions, or ideas held by my current employer.

```
/end disclaimer
```


Responsible Disclosure?

"It cannot be too earnestly urged that an acquaintance with real facts will, in the end be better for all parties."

A. C. Hobbs, *Locks and Safes: The Construction of Locks*. 1853

Introduction

- Disclosure (“responsible”) or otherwise is divisive
- Vendor and researcher expectations are different
- There are a host of legal implications
- Developing an understanding of what to disclose, when, and to whom is vital

Some History

- Human beings have always kept and shared secrets
- Most discussions on vulnerability disclosure refer back only to the locksmith debate of the 19th century
- Whether or not to disclose (and indeed what to disclose) is one of the oldest issues in moral history

Some more History

- The disclosure debate (in relation to computer security) started over ten years ago in the early 90's
- CERT (Computer Emergency Response Team) = the ivory tower
- In 1993, Bugtraq was unleashed out of a growing sense of frustration with CERT

Recent History

- The conflict between responsible and full disclosure rumbles on
- From 2001 (Excite@Home) Adrian Lamo worked with a variety of vendors – but still found himself on the wrong side of the law
- In 2003, David and Mark Litchfield (NGS) were bought into conflict with CERT
- In 2004, Michael Zalewski unveiled the MangleMe fuzzer. In 2006, he courted controversy by posting the MSIE (mshtml.dll) OBJECT tag vulnerability without communication with Microsoft

Recent History

- In 2005, Cisco leant on ISS to prevent Michael Lynn's Blackhat talk on Cisco IOS; because it was, according to them "information that was illegally obtained and violated our intellectual-property rights". Lynn resigned and did it anyway.

- Earlier this year, HID (who make RFID badges – take note Mr Laurie) threatened Chris Paget of IOActive into silence at Blackhat DC regarding his planned talk on an RFID cloner (again, citing infringement of intellectual property). The talk was cancelled.

Today

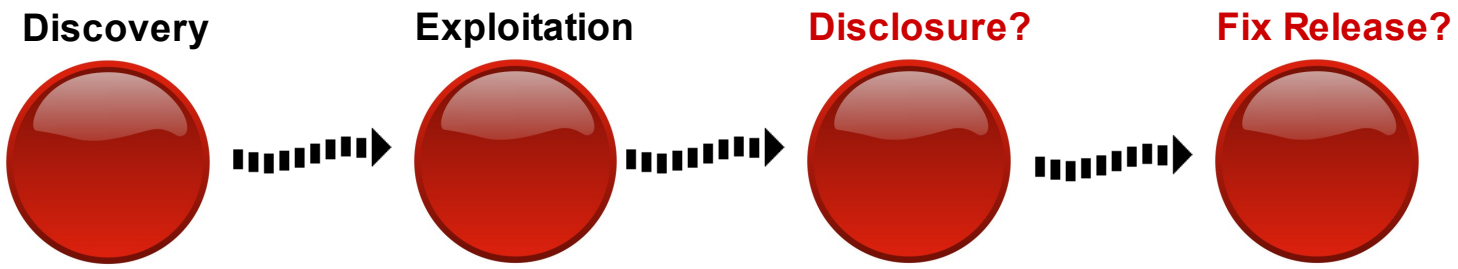
- The OIS (Organisation for Internet Safety) was formed in 2003 by a number of vendors in reaction to Full Disclosure
- Oracle and researchers have been battling it out for years, with CSO Mary Ann Davidson wishing to silence researchers – other vendors may well agree…(*cough* MS *cough*)
- Private companies (iDefence, Tipping Point, etc.) now pay for undisclosed security vulnerabilities – Security through obscurity = cash?

Current Disclosure Practices

- Full – Tell the world before the vendor
- Responsible – Tell the vendor before the world
- Profit driven – Tell a paying third party; hope they tell the vendor and the world
- Non – Tell no-one

A Vuln is Born

- Every vulnerability that is discovered by a researcher (as opposed to a ‘blackhat’) has a lifecycle:

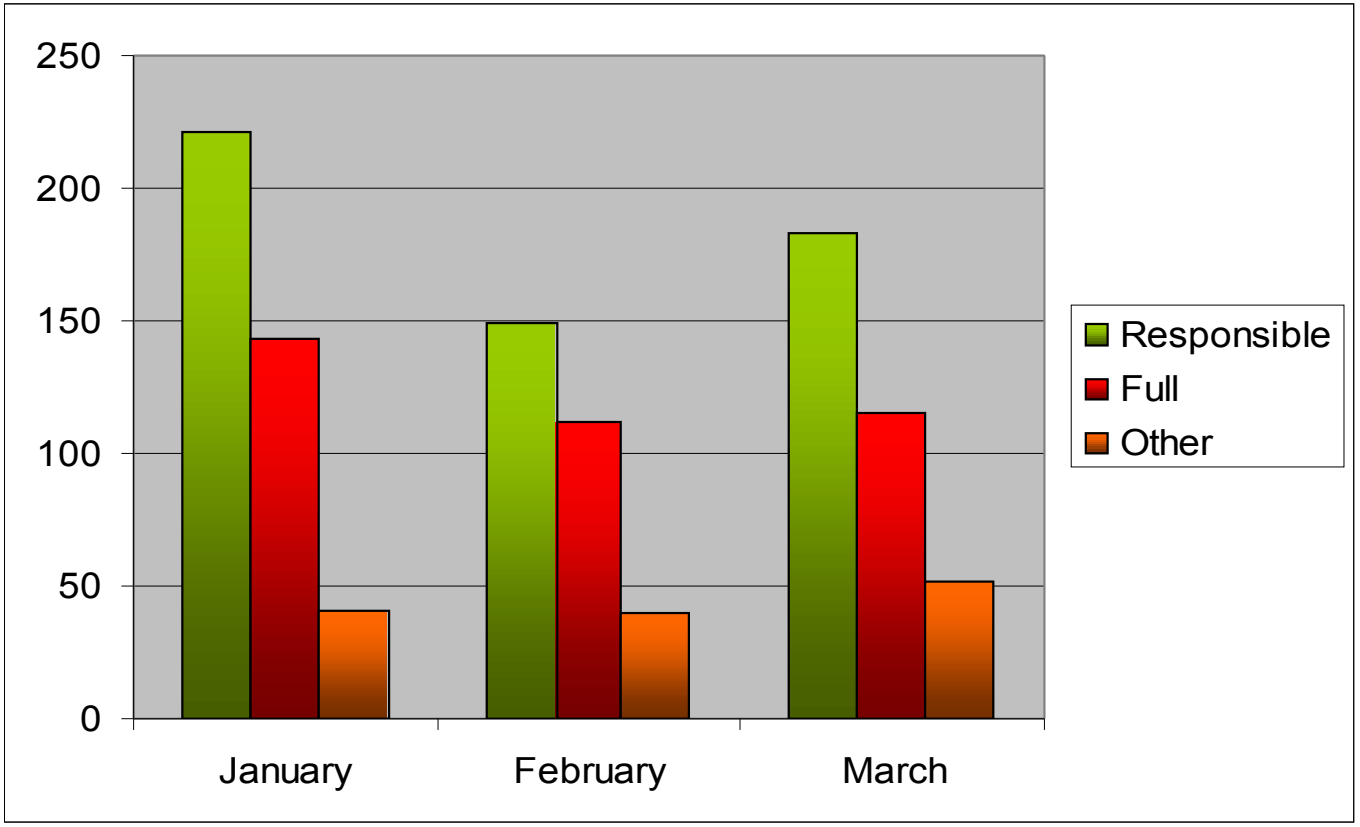


A Vuln is Born

- What happens between exploiting and disclosing a vulnerability is where the disclosure process comes in
- Researchers may choose to alert a vendor before publication, they may choose to force the vendors hand by a public release, or they may retain vulnerability details for potential later malicious use
- The choices made by researchers all rely on the colour of the hat, and the size of the ego…

Lies, Damn Lies, and Stats

Number of Vulnerabilities by Disclosure type: Bugtraq 2007



What the Stats show…

- Overall Bugtraq appears to have moved towards a responsible disclosure model?

- Partial disclosure is still not a popular form of disclosure

What the Stats don't show…

- Included in Full disclosure statistics are those vulnerabilities that make no mention of either contact with vendors or patches
- Included in Responsible disclosure statistics are postings from vendors, 'Others' includes proved false positives
- Obviously one statistic that couldn't be included in this analysis was the number of zero days in existence…
- No differential between enterprise level vulnerabilities and those in 'friend of a friend' software packages / shoddy XSS

"Best" Practices

- Best industry practice for vulnerability disclosure arguably dates back to the 'Full Disclosure Policy (RFPolicy) v.2.0' published by Rain Forest Puppy in 2000

- Most corporate guidelines for disclosure acknowledge this document as an important source (although NTBugtraq disclosure guidelines http://www.ntbugtraq.com/default.aspx?sid=1&pid=47&aid=48 predate it by a year)

Disclosure according to RFP

- Researcher (Originator) contacts vendor by email (Date of Contact)
- Vendor has five days to respond from DoC, if no response, publish
- Researcher has to help replicate vulnerability with vendor
- If anything in process takes more that five days – publish
- Publication should wait until patched, and be joint release between vendor and researcher

Problems with RFP Disclosure policy

- Five days is a long time for a small vendor with one product. For a major vendor with enterprise level software this is nothing
- Communications can break down – the five day window doesn't provide much room for haggling
- Disclosure should be about collaboration, setting such time limits may make the process unnecessarily confrontational

Current ‘corporate’ policies – ISS X Force

- Same model as RFP but with no time limitations
- Caveats concerning disclosure (e.g. disclosure will occur if the vendor is ’unresponsive’, the media reports the vulnerability, active exploitation of the vulnerability is observed, etc.)
- Process is defined; timescales are not (in July 15, 2004 revision)

Current ‘corporate’ policies – Symantec

- Contact with vendor. Response to be received with seven days – or publish
- Contact to be maintained every seven days – or publish
- Issue to be resolved in thirty days, or publication unless “good faith effort” is made by vendor
- For unresponsive vendors, grace period of thirty days *may* be granted prior to publication (Disclosure policy – January 2006)

‘Corporate’ policies - Conclusions

- Wide variety of timescales, details released, and process
- No consistency in either research company policies or indeed in how vendors should respond
- All security research companies are interested in being ‘first to market’ with vulnerabilities – disclosure policies seem to be a moveable feast…

This is all *really* interesting, but…

- As a member of the security industry, you have to know about disclosure
- Vulnerabilities are not hard to find – enterprise level vulnerabilities are a different story!
- What happens if you find a high risk enterprise level vulnerability during the course of a client engagement??

Vulnerability + Engagement = ?

- All depends on the agreements in place between researcher and client
- Does your company have a disclosure policy? If so, who carries legal liabilities that may be involved?
- First duty is to complete engagement *unless* vulnerability is so severe as to cause widespread damage to enterprises
- Process and agreement led – your responsibility is to know both…

Dealing with the client

- In anything other than exceptional circumstances – duty of care is to the client
- Who takes ownership of the vulnerability that comes from an engagement?
- Vulnerability details may need to be sanitised so that the client is not exposed to danger

Dealing with the vendor

- First contact is vital – be technically specific and non-confrontational
- Follow guidelines in place by your company policies (if they exist!)
- Offer mitigation advice if appropriate
- The process is one of collaboration – not about personal glory
- Drop the ego!

A less than perfect world?

- The vendor will probably not appreciate your efforts
- The vendor may become unresponsive
- The vendor may appear to be technically obtuse
- The vendor may not have experience in dealing with vulnerabilities
- The vendor may wish to communicate insecurely (unencrypted email etc.)
- You might be sued… You might go to jail… You might lose your career

Less than loose lips…

- Historically there has been a substantial gap between how researchers are perceived by vendors and how they perceive themselves
- For a number of years now, researchers have been seen at best a minor consideration, and at worst maliciously inspired miscreants
- This attitude is changing (slowly) but remnants of old combativeness may still remain (especially true for those researchers not protected by a corporate shield)

Less than loose lips…

- How do you overcome the combativeness or silence that may greet the news of you latest vulnerability?
- Could react according to RFP and other guidelines and force a response by Full disclosure
- Not a great idea!
- Increasing calls to make researchers responsible legally for publishing vulnerability data

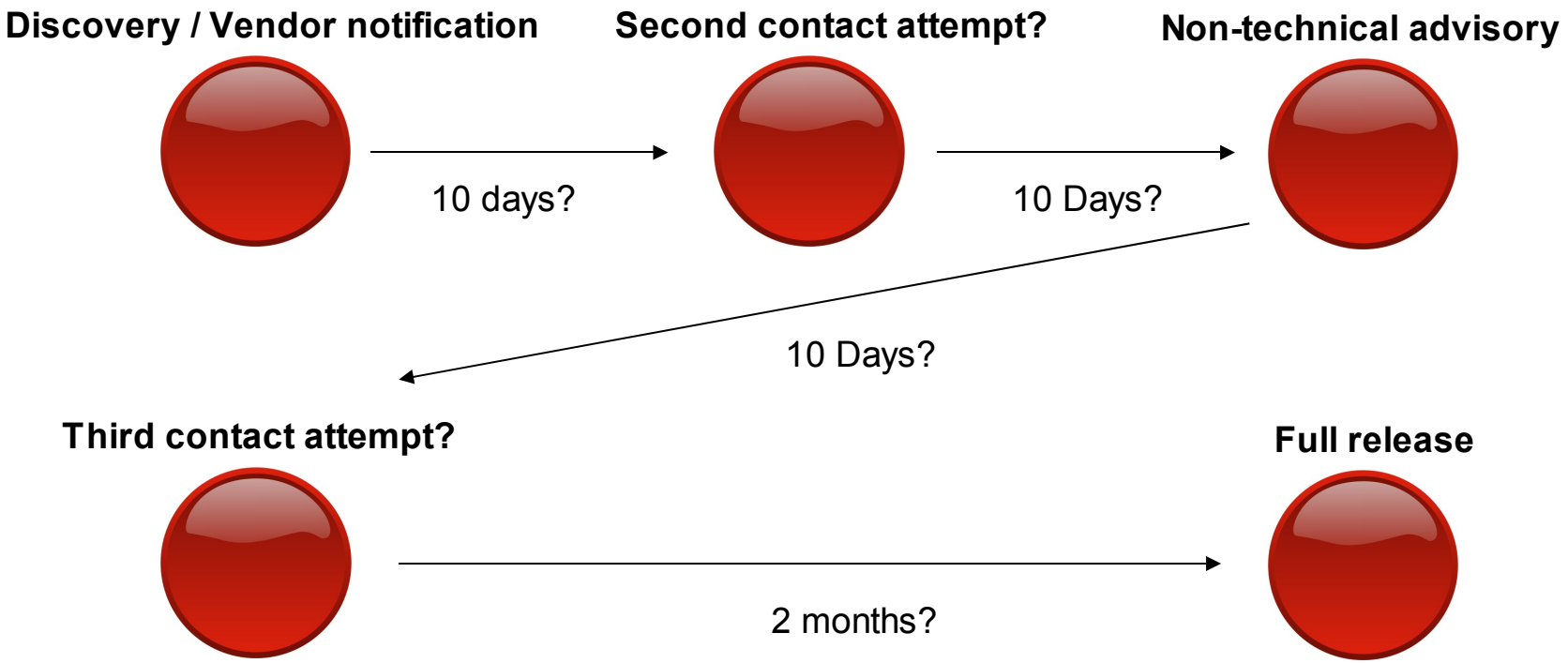
Less than loose lips…

- Politically the climate in Europe and the US has changed where ‘hacking’ can now be considered an act of terrorism. Can’t be long before full disclosure is seen as a terrorist act?
- Full disclosure *may* force the vendor to respond – it will definitely expose enterprises to an increased level of risk
- So, other than accepting the decrees of a security naïve vendor, what can the researcher do when faced with resistance?

Vaulting the stone-wall

- Researcher reports vulnerability securely to vendor
- Vendor ignores researcher, or communication breaks down
- Researcher attempts second contact (detailing intention to publish)
- Researcher publishes non-technical advisory (with reasonable opportunity of time for vendor response – attempt vendor contact)
- Following time expiration researcher publishes technical advisory (without exploit code)

Vaulting the stone-wall



And this differs how?

- Unlike RFP / most Corporate policies first response is not full disclosure
- Generic details, followed by technical advisory with no exploit code that can be misused
- Multiple opportunities for vendor response – reduced legal liability?
- Timescales need to be considered – three month window?

Problems

- The legal responsibility and liability remains with the researcher (or company)
- Still creates combativeness between research and vendor communities
- The lack of exploit code, although it may prevent malicious use, may also impair legitimate continued research
- Research is published – but where's the patch / fix?

Solutions?

- Vendors and researchers operating according to their own rules (OIS vs. RFP)
- Maybe CERT wasn't such a bad idea?
- Mediating group, that includes vendors, research companies and individual researchers?
- The ends may differ but isn't the aim the same?

Easing the process: Vendors

- Security contacts should be easy to find
- Timely security response processes should be in place
- Communication with researchers should occur securely
- Researchers should receive credit not damnation
- Customers should be informed that vulnerabilities have been discovered and provide temporary workaround / timescale to fix

Easing the process: Researchers

- Give the vendor the benefit of the doubt
- Communicate securely with the vendor where possible
- Provide any technical details requested in a timely manner
- Provide assistance with mitigation / resolution if appropriate
- Inform the vendor of the methodology / timescales being followed
- Don’t put personal ego before enterprise security

Equal parts bravado and stupidity

- The days of Full disclosure are behind us?
- Vulnerability purchasing companies and schemes can help separate the researcher from the vendor – this is not motivated by altruism however…
- Recent events (Lamo, Cuthbert, McCarty, Paget, Lynn et al) show that the reporting vulns can be a risky and potentially damaging process
- Because of arguably non-malicious attacks, researchers have lost their career credibility and gone to jail

Risky Business

- As no-one can decide what to report and when, and the risks posed by annoying the wrong parties are severe, why bother reporting anything?
- Silence does not increase security
- Third party commercial vulnerability purchasing companies do not exist to increase security – they exist to make money
- Disclosure helps increase security levels (unless it's Full in which case the effects can be quite the reverse)

Risky Business

- Non disclosure is not an option to any ethical researcher
- Disclosing vulnerability details without giving the vendor adequate response times is also unacceptable
- Security research is fraught with risk and legal implications – and it remains the responsibility of the security professional to decide their own limits and actions

Who wears the pants?

- In recent comments at Schmoocon, ex MS (and now Mozilla) security something or other, Window Snyder claimed that “the researcher has all the power”
- Couldn’t be further from the truth (I have no team of legal specialists – how about you?)
- Dave Aitel, claimed that responsible disclosure was a ruse, and that the alternative was to sell your wares to him…

Who wears the pants?

- The simple fact is vendors are getting more and more twitchy
- It may be the license agreements for software are not well defined (your ‘acceptable use’ and theirs might differ) and arguing that legally is tricky sometimes
- Vendors are thus using the stick of intellectual property more and more
- At the moment he with the biggest legal staff wins…. Which is frankly asinine and has negative ramifications for all…

Putting away the toys

- Self determination doesn't work
- The computer security 'industry' has matured significantly over the last few years – needs to start acting its age?
- Is the goal to improve security for all – or turn a fast buck?
- Disclosure processes need to be regulated from within and without to ensure that vendors and eager lawyers can't target individual researchers, and that irresponsible researchers don't drag us all down to their level

Scary thoughts

- The research community needs regulation and agreed guidelines?
- Regulation cannot come from .gov (which may be the way it is headed)
- Regulation cannot come solely from industry (OIS anyone?)
- Regulation has to come from the community?
- If the disclosure models and practices don't change – security won't ever be increased (it's hard to conduct research from a cell…)

Propping up the sky?

- When legitimate researchers go to jail, and zero days are being used in anger – something isn't working
- Responsible disclosure is so loosely defined now, that it may not ever be workable?
- A solution needs to be found – and can arguably only be found in collaboration
- Time to evangelise to vendors and beyond, as well as trying to clean our own house?

Thanks

- Questions?
- Comments?
- Random abuse?
- Too bored by this talk to comment now? – get in touch at www.clappymonkey.com or clappymonkey@gmail.com

Acknowledgements

- My boss; for the time
- My colleagues (past and present); for putting up with me
- Melanie Flynn
- Researchers and vendors everywhere; for fighting the good fight