“Monitoring Exploit Sales & New Responsible Disclosure”

(required title)

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Berlin

14th February 2013

NPL
National Physical Laboratory

Regulating zero-days

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

NPL
National Physical Laboratory

Berlin

14th February 2013

What is a “zero-day”

- A zero-day is an exploit for a previously unknown vulnerability
  - you have 0 days in which to deploy a patch
- It is commonplace for the first sign of a vulnerability to be an exploit “in the wild”
- All sorts of different types of vulnerability
  - input data handling buffer overflow
  - directory traversal (../../../etc/master.password)
  - packet of doom (Juniper, Intel 82574L etc)
  - input parsing (From: <script>….)
  - XSS (<html>Your input <script>…</script> was an error</html>)
  - etc. etc.
- However, note that zero-days not necessarily effective
  - external filters can discard traffic containing exploits
  - randomness can prevent generation of universal payloads

Current disclosure schemes

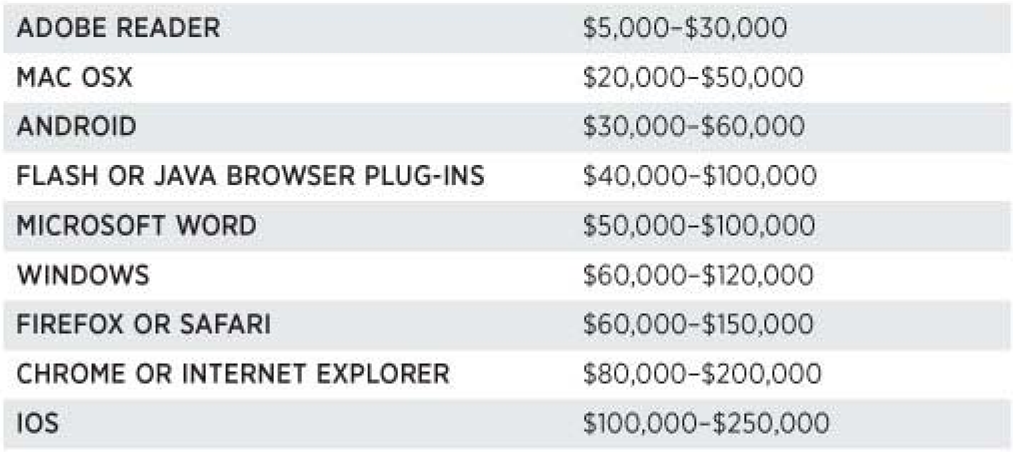
- Dear World, I have found a problem in vendor’s product
  - so-called “full disclosure” – puts immediate pressure on vendor
  - might form centrepiece of a BlackHat talk
  - makes you famous and may get you consulting work
- Dear Vendor, I have found a problem in your product
  - so-called “responsible disclosure”
  - vendors may not act, so sometimes a 30(etc) day deadline is set
  - problem may be multi-vendor; CERT-CC often handles this
  - it is a Big Mistake for vendors to forget to credit the finder
- Dear Criminals, would you like to buy an exploit for this product
  - part of the specialisation of the “underground economy”
  - $5000 for a Java exploit (Jan 2013)
- Dear Prime Minister, I would like a medal for helping the spooks
  - or a nice car, or a cushy job in a warm building…

Bug bounty programmes

- Mozilla (2004)
  - currently pays $3000 for browser security bugs
  - has paid out $750K over 8 years
  - now followed by Google ($1.5M paid), Facebook and many others
- iDefence (2003) & Tipping Point (2005)
  - pay for bugs in major products
  - idea is that their customers get protected at an early stage
  - economic analysis shows can be sub-optimal (see Choi et al)
- Schechter, Osman & others considered the marketplace
  - perhaps prices paid for bugs would signal relative security ?
  - hasn’t really panned out that way

The new breed of purchasers

- Military/industrial complex now purchasing bugs for a premium
- Greenberg (Forbes, March 2012) had a pricelist:



ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

- Purchasers are spy agencies, security product vendors (who want a good demo) and penetration testers (who want to impress potential clients)
- Google, iDefense and others report fewer submissions…
  - though of course better internal testing means fewer bugs to find…

Suppose we regulated the zero-day sales

- Parallel is with arms control – and that mainly works
  - albeit a weak parallel, Krupp doesn’t operate out of a bedroom
- Can prevent sales to undesirables
  - bona fides of purchasers can be checked (so can exclude mafias)
  - sales must be in line with foreign policy (no pariah states)
  - require that usage does not infringe human rights
- Can have first dibs on the good stuff
  - c.f. the exceptions in national patent laws
- Legitimate businesses would comply
  - otherwise whistleblowers would hold them to ransom!
  - rules unlikely to affect who they actually sold to
- Presumably vendor programmes would be exempted
  - otherwise how can you run Pwnium ever again?

Regulating the market – cons

- Legitimises trade in the “bullets of cyberwar” (Soghoian)
- Will be ineffective and ignored (can’t stop trucks at the border)
- Risk that law will merely result in prosecuting the ignorant
  - and those who don’t want to comply will hide (Tor etc.)
- West is not the main source of zero-days, so no overall effect
- Report will be (discoverable) evidence of breach of contract with vendor (finding zero-day not covered by Art6 2009/24/EC)
  - vendor could use FOI legislation to obtain details and reduce cost of their bug bounty programme!
- Local spooks will require that sales to them to be exempt
- Regulator will accumulate a very valuable database
  - and may not have the skills to protect this data
  - no exact details, but hints may well suffice (e.g. Kaminsky bug)

http://www.cl.cam.ac.uk/~rnc1

http://www.lightbluetouchpaper.org

Dr Richard Clayton

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

NPL
National Physical Laboratory