

Offset	Topic
00:17	<ul style="list-style-type: none"> <li>• <b>Intro</b></li> </ul>
01:56	<ul style="list-style-type: none"> <li>• <b>Security Alerts</b></li> </ul>
02:15	<ul style="list-style-type: none"> <li>• New counter measure against worms <ul style="list-style-type: none"> <li>• <a href="http://rss.slashdot.org/~r/slashdot/eqWf/~3/304871205/article.pl">http://rss.slashdot.org/~r/slashdot/eqWf/~3/304871205/article.pl</a></li> <li>• New research from Ohio State University</li> <li>• Infected machines start scanning a wide variety of other systems</li> <li>• Looking for likely new targets to infect</li> <li>• Common sense indicates unusual volume of scans indicates an infection</li> <li>• A good heuristic for taking such machines off the net and diagnosing</li> <li>• Researchers looked at relationship between how long an infected system was allowed to actively scan and probability a virus would spread</li> <li>• Scans and scan-like activity are also part of normal traffic</li> <li>• What is the best cut off point, especially for automated response?</li> <li>• Researchers developed a model and tested against Code Red and SQL Slammer</li> <li>• Turns out key value was well beyond what occurs on a normal network</li> <li>• But this threshold was very quickly reached by infected machines</li> <li>• Achieved some impressive results</li> <li>• Recommend it as a complementary measure alongside other protections</li> <li>• Similar to work also done at Pennsylvania State University</li> <li>• Sounds like this is a network level technique, so more effective for ISPs, companies and schools</li> </ul> </li> </ul>
04:56	<ul style="list-style-type: none"> <li>• Mozilla contemplates successor to same origin policy, Site Security Policy <ul style="list-style-type: none"> <li>• <a href="http://rss.slashdot.org/~r/slashdot/eqWf/~3/306307630/article.pl">http://rss.slashdot.org/~r/slashdot/eqWf/~3/306307630/article.pl</a></li> <li>• Idea is in the very earliest of stages, discussion</li> <li>• No specification, yet, though there is some experimental code</li> <li>• Code is in the form of a Firefox extension</li> <li>• Intended to spur discussion and lead to a full proof of concept</li> <li>• Effort is a response to the rise of XSS and XSRF attacks</li> <li>• Intended to complement, supplement application level security, not replace it</li> <li>• Looks like an expansion of same site origination policy</li> <li>• Server gets to declare white lists for different kinds of sources and targets</li> <li>• So intend for a safe way to allow two sites/services to call each other's scripts, content</li> </ul> </li> </ul>

## Offset

## Topic

- Uses simple HTTP headers, means non-capable browsers would just ignore
- Requires browsers to correctly adhere to policies
- Unclear yet how they will deal with spoofing of policy information itself
- Also unclear whether a system admin or an application developer would be responsible for setting policy
- Not sure how to popularize this to end users
- Will really rely on uptick by end users
- Hopefully we can get to proof of concept stage quickly as a live demonstration may make the operation of SSP more clear

09:50

### • News

10:03

- Princeton paper on government transparency
  - <http://feeds.feedburner.com/~r/techliberation/~3/303046023/>
  - David Robinson, Harlan Yu, William Zeller, Ed Felten
  - To be published as a final draft in Yale Journal of Law and Technology this Fall
  - The policy recommendation is simple
  - Current policy focuses on governmental web sites
  - These are expensive and prone to falling out of date
  - Nettle of regulatory compliance makes developing such sites difficult if not impossible
  - Paper suggests instead that government provide open data feeds
  - Third parties could take over building the human facing sites
  - Argues that competition would see many different, better ways into the data
    - Some of this is happening, anyway, just at higher cost
    - Govtrack.us, Maplight, Sunlight
  - Realistic enough to recognize not all areas of government would benefit
  - Cost savings in most popular could offset burden of maintaining feed and site for less popular
  - The engineer in my likes this idea
  - I even like that they extrapolate out to a browser or browser feature for perusing this data directly
  - I am concerned that some requirements are glossed over
  - Accessibility, at least, seems to be a big one
  - Would third parties have to comply, which raises their cost?
  - If not, then would that not disenfranchise some?
  - Unique issues to private parties are overlooked
  - Common carriage versus private forum
  - This is confusing enough for purely private plays
  - Detecting bias in this scenario could be difficult

## Offset

16:02

## Topic

- If end user choice is limited, how can a consumer really use Free Speech to deal with any issues?
- I think this is an earnest beginning, but it will clearly need more thought
- At a minimum, open data feeds alone will not be enough in the short term or for some aspects of government
- Subsidizing a browser or browser plugin could be an interesting compromise to traditional web sites
- This is some of early thinking from Robinson, Felten; look forward to more
- The real ACTA threat
  - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/302908867/20080602-the-real-acta-threat-its-not-ipod-scanning-border-guards.html>
  - ACTA is a trade agreement, negotiated in private
  - Nominally it is an anti-counterfeiting trade agreement
  - Would apparently include piracy measures in its scope
  - Would be between US, Canada, the EU, and Japan among others
  - Recently a document was leaked outlining the draft
  - There are implications that its scope would be broader
  - I have heard of ACTA before though not very familiar
  - Even earlier references seemed to be low key
  - Ars confirms this, that the treaty has been public knowledge since last year
  - Information has been scant
  - Agreement is bypassing the World Trade Organization and the World Intellectual Property Organization
  - This would eliminate some of the leeway that has been allowed with past WIPO treaties
  - There is also the suspicion that later signees would not get any negotiating room
  - There apparently is no actual draft as of yet
  - Leaked document is a "discussion paper"
  - Much hand wringing in the press, theories about border search and seizure for copyright infringement on digital devices
  - Discussion paper is not a draft, suggest provisions that might make it into a draft
  - Ars analysis yields much blander customs language, though it would amount to new powers
  - Really trouble provisions target hubs like Pirate Bay and seek to spread DMCA safe harbor under takedown provisions more broadly
  - The piracy hub language takes out consideration of commercial gain, seems to speak directly to pirate trackers, other non-profit entities

<u>Offset</u>	<u>Topic</u>
6/2/08	<ul style="list-style-type: none"> <li>● Under the ISP provisions, would also perhaps erode judicial oversight in acquiring subscribe information when infringement is suspected</li> <li>● At its heart, this seems like another trade play to spread maximal control we've been seeing in the US globally</li> <li>● EFF on ACTA <ul style="list-style-type: none"> <li>● <a href="http://www.eff.org/action/sunlight-acta">http://www.eff.org/action/sunlight-acta</a></li> <li>● Some more history</li> <li>● Also a link to take action</li> </ul> </li> </ul>
6/3/08	<ul style="list-style-type: none"> <li>● Patry on ACTA <ul style="list-style-type: none"> <li>● <a href="http://williampatry.blogspot.com/2008/06/acta-call-to-arms-no-more-secret.html">http://williampatry.blogspot.com/2008/06/acta-call-to-arms-no-more-secret.html</a></li> <li>● Outlines why making copyright a trade issue s a problem</li> <li>● US Trade Representative historically has always pushed for more copyright</li> <li>● Has not always had the power to enact, however</li> <li>● Under the US Constitution, that power is meant to reside solely with Congress</li> <li>● ACTA would reshape IP law under the USTR and do so in private, without the scrutiny a Congressional action would involve</li> <li>● Biggest objection is to closed proceeding, rather than any specific provision</li> <li>● Does mention another provision supposedly in the draft, from a trusted source</li> <li>● Will apparently include ISP filtering measures</li> <li>● Seems consistent with the Ars discussion of changes to information gathering, ISP involvement</li> <li>● Patry doesn't dwell on it, preferring to stick to the main issue</li> <li>● Other sites are already picking up on it, though</li> </ul> </li> </ul>
22:37	<ul style="list-style-type: none"> <li>● Ease of spoofing copyright infringement online <ul style="list-style-type: none"> <li>● <a href="http://bits.blogs.nytimes.com/2008/06/05/the-inexact-science-behind-dmca-takedown-notices/">http://bits.blogs.nytimes.com/2008/06/05/the-inexact-science-behind-dmca-takedown-notices/</a></li> <li>● Abuse of DMCA takedown has been speculated before</li> <li>● The investigative techniques of the RIAA has repeatedly been called into question</li> <li>● This is the first systematic study of the problem</li> <li>● Tadayoshi Kohno, Michael Piatek and Arvind Krishnamurthy undertook a detailed study</li> <li>● Two studies, actually, in May and August of last year</li> <li>● Originally were looking at who participates in BitTorrent traffic</li> <li>● Received so many false takedown notices, launched this study, including data from the fist</li> <li>● Launched monitoring agents, were not downloading anything</li> <li>● Received more than 400 takedown requests</li> <li>● Seem to confirm poor practices and even intentional framing</li> </ul> </li> </ul>

- Concluded enforcers are only considering IP addresses, not actual content
- Also speculate enforcers and ISPs are being driven more and more to automation to deal with volume
- Did not even have to use IP spoofing
- Explain a false positive based on timing between tracker requests and DHCP leases
- Also, demonstrate an attack using an extension to BitTorrent meant to help with proxies and NATing firewalls
- Their demonstration involved framing print servers, which received multiple take down notices
- Researchers hope their paper will help bring about more open-ness in what, exactly, enforcers are doing
- Give feedback to P2P users, too, suggest more effective ways to identify monitors
- Prove black lists are no good but explain simple analysis for spotting monitors
- I am encouraged that this is a disciplined study
- Also that it was picked up by mainstream press, although it is NYT's tech blog
- Trends in paper may also push enforcers more to 10x-100x more expensive content analysis or, more likely, to keep coopting ISPs for DPI
- Felten on DMCA take downs based on inconclusive evidence
  - <http://www.freedom-to-tinker.com/?p=1298>
  - Suggests that a soft "warning" might be warranted by the lightweight monitoring detailed in the paper
  - Might even be an effective deterrent with the understanding of the threat of more conclusive investigation
  - Deconstructs the letters, too
  - Points out how they do not jibe with the studies findings
  - Speculates a little beyond cost as to why rights holders don't do more in depth verification
  - Claim positive infringement in cases where that is impossible
  - Means that takedown notices are effectively little more than warnings
- Reverse engineering the brain
  - <http://www.spectrum.ieee.org/print/6268>
  - Profile of David Adler's work
  - Using advanced imaging to map out smallest neurological structures
  - Project at a campus called Janelia Farm, part of Howard Hughes Medical Institute, is courting Adler
  - Their goal is to understand the human brain
  - To answer that core question of neuroscience, how does the brain do what it does
  - Starting with a fruit fly brain

## Offset

## Topic

- Proceeding from the assumption that the difference to a human brain is quantitative, not qualitative
- Very similar to reverse engineering an integrated circuit
- Fruit fly brain is more complex than an IC but not by a huge amount
- Neurons are more analog, though, unlike an IC, hence the need for Adler's imaging
- Highly multidisciplinary team to bridge that difference between simply logical circuits and neural wiring
- Article details the challenges, continuing to contrast to IC reverse engineering
- Sample preparation is tricky, given the organic nature
- Amount of raw data is immense, especially with pushing the cutting edge of imaging with Adler's help
- Looking to use machine learning to deal with data glut
- Characterize the images faster to cut down on what needs to be stored
- Article entertains speculation of building thinking machines with these "wiring diagrams"
- Regardless, this is some pretty hefty basic science
- Benefits are not hard to appreciate, from understanding disease to various aspects of human cognition
- Wouldn't necessarily need to fully understand the human mind to realize these benefits
- Also the technological innovations, like improvements in imaging and data processing
- Sort of a Manhattan project for neuroscience

34:49

- `tail -f`

35:09

- Media Defender defends syn attack on Rev3
  - <http://feeds.wired.com/~r/wired/topheadlines/~3/303096647/mediadefender-d.html>
  - CEO claims it didn't realize who they were targeting
  - Claims the tracker in question was serving a large volume of pirated content
  - Basically doesn't sound like MD is owning up to anything
  - Louderback's point that MD should have investigated and tried contact is still valid
  - His hyperbole about air traffic control is a bit unwarranted
  - It is enough that MD took out the operations of a legitimate business, beyond the scope of taking out a pirate tracker
  - With the FBI definitely investigating, there may be more to come

36:19

- DTrace improved in latest OS X update
  - [http://blogs.sun.com/ahl/entry/apple\\_updates\\_dtrace](http://blogs.sun.com/ahl/entry/apple_updates_dtrace)
  - Original post described experiments that showed some DTrace code failed

## Offset

## Topic

- Tracked it down to happening when certain applications, like iTunes, were running
- DTrace is a development tool original developed by Sun but adopted by others
- Apple shipped it with Leopard prompting Adam Leventhal's investigation
- Recent update, 10.5.3, improves DTrace behavior, Adam shares some empirical results
- There are still some issues, though Adam doesn't lay these at Apple's feet, per se
- One that he does is that application names are still redacted
- Correctly points out that other tools, like Activity Monitor, show these applications by name
- Asks whether revealing just application names in DTrace would be any different

38:40

### • **Outro**

- Contact me
  - Email to [feedback@thecommandline.net](mailto:feedback@thecommandline.net)
  - Web site at <http://thecommandline.net/>
  - IM to [command.line@skype](mailto:command.line@skype)
  - Listener comment line is 240-949-2638
  - [del.icio.us](http://del.icio.us) tag is "for:cmdln"
  - <http://twitter.com/cmdln>
- I'd like to thank [libsyn.com](http://libsyn.com) for AAC hosting and Wouter de Bie for MP3 hosting
- These notes and the show audio and music are covered by a Creative Commons license
  - <http://creativecommons.org/licenses/by-nc-sa/3.0/us/>
  - Attribution, non-commercial, share alike