

Offset	Topic
00:17	<ul style="list-style-type: none"> <li>• <b>Intro</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Father's Day               <ul style="list-style-type: none"> <li>• Interest in computers sparked by my dad</li> <li>• Logical, analytical skills inherited from, fostered by Dad</li> <li>• Common joke growing up, encoding ages on birthdays in different bases</li> <li>• Taught me many fast math tricks</li> <li>• Looking to share many of my talents, skills with my kids</li> <li>• Already taught them to count in binary</li> </ul> </li> </ul>
04:57	<ul style="list-style-type: none"> <li>• <b>Security Alerts</b></li> </ul>
05:16	<ul style="list-style-type: none"> <li>• Updated ransomware bumps up encryption strength               <ul style="list-style-type: none"> <li>• <a href="http://blog.washingtonpost.com/securityfix/2008/06/ransomware_encrypts_victim_fil.html">http://blog.washingtonpost.com/securityfix/2008/06/ransomware_encrypts_victim_fil.html</a></li> <li>• Malware that encrypts files on target machine, then issues ransom notice are relatively new</li> <li>• The one in the article is the latest</li> <li>• Identified by Kaspersky Labs as Gpcode</li> <li>• There have been several versions of Gpcode</li> <li>• Each has strengthened the crypto, each has been cracked</li> <li>• This version boasts a 1024 bit key</li> <li>• Seems to be not very common, Krebs speculates mostly in Eastern Europe, Russia</li> <li>• Offline back ups are suggested in the comments</li> <li>• If all the malware can do is grab one copy, limits damage</li> <li>• Kaspersky is making noises on their forums about a distributed project to crack</li> <li>• Implies there is one key or a small number of keys</li> <li>• What happens in someone pays the ransom and distributes the decryptor?</li> <li>• That last also from the comments</li> <li>• Commenter clarifies, the longer key is a single one, used to encrypt a wider range of smaller keys, used to do actual encryption</li> <li>• Decryptor submits encrypted key to attacker's server, which decrypts and sends back</li> <li>• Does form a target for law enforcement, though</li> <li>• What guarantee that payment will net a real decryptor or one that is not itself laced with more malware?</li> <li>• Past breaks were as much about errors in implementation</li> <li>• Latest version seems improved but may still be possible to exploit a flaw</li> <li>• Distributed computing to defeat stronger ransomware</li> </ul> </li> </ul>

## Offset

## Topic

- <http://rss.slashdot.org/~r/slashdot/eqWf/~3/309685900/article.pl>
- Their invitation is just a sharing on the public key
- Doesn't appear to be any further coordination
- Despite coverage, no code written and shared
- Quite clearly asking the community for that
- Ransomware resisting crypto cracking
  - <http://www.securityfocus.com/news/11523?ref=rss>
  - Security industry has responded skeptically
  - Schneier states its just not a feasible problem to brute force
  - Others point out it is not a permanent solution
  - Author can re-issue with different, uncracked key
  - Some claim the project is just a publicity stunt
  - Company has clarified, looking for help to find flaws
  - Forum posting says otherwise, just shared keys
  - Supposed other already claiming plans to up key strength to 4096-bit
  - Also apparently planning to turn into full blown virus, using latest techniques

13:30

### • News

13:44

- The Piracy Bureau on inevitability of copyright failure for digital media
  - <http://feeds.feedburner.com/~r/boingboing/iBag/~3/308974135/swedish-pirate-burea.html>
  - Rasmus Fleischer, PhD student and co-founder of The Piracy Bureau
  - <http://en.wikipedia.org/wiki/Kopimi#kopimi>
  - Other members founded The Pirate Bay
  - The Piracy Bureau dedicated to fighting current views on IP, favor instead free, open sharing
  - Fleischer notes a generalizing trend
  - From text to works to tools
  - Focuses on the later
  - Arms race between industry and desire for content
  - As a law or technology is circumvented a new bill is introduced
  - Internet, software erasing differences between formerly distinct media
  - Explores the arbitrary difference between downloading, stream as an example
  - Also hints at issues with reverse copyright theory Patry has explained
  - Technology allows unintended uses, opportunities
  - This cascade of legislation is trying to stifle or capture this open change
  - Implies this will accelerate

## Offset

## Topic

20:03

- As a function of how copying is fundamental to computers
- Separates ease of copying from Internet, mentions darknet
- Distribution will flow where and how it can, the key issue is the ease of copying
- Touches on Kelly's essay, Better than Free
- Suggest we need more emphasis on where real value can be derived with the super abundance digital copies afford
- Shares the example of Getty Images which has been failing for years
- Attributes this to abundance created by cheap digital cameras
- Un-copyable quality is feel of real time presence, which Getty's large archival database didn't provide
- Folds in ACTA and the push to filtering
- Questions the vague definition of operator and of service provider
- Suggest there may be a minefield here, may be interpreted as libraries, individuals
- His ultimate point is this worsening trend is an attempt to capture a world that is already gone
- If industry doesn't wise up, this will continue to get worse
- Counter pressures, like P2P and darknets will also grow
- Doesn't suggest a strong way forward, rather implies that the more time wasted on "universal copyright", the longer we have to live with gray areas
- What is at stake with white space devices
  - <http://arstechnica.com/news.ars/post/20080608-if-white-spaces-fail-we-dont-have-that-many-chances-left.html>
  - Much of the past coverage has centered around specific devices
  - Most of them have not worked as advertised
  - Opponents fear interference with licensed uses, in particular broadcast
  - At issue are the "white spaces" or unused TV band spectrum that may vary by market
  - Highly desired for range and propagation
  - For those seeking to build a wireless broadband alternative, very attractive
  - WiFi just can't be pushed far enough to serve large areas
  - However the success of WiFi as an unlicensed spectrum uses is a strong indicator of what could be done with better spectrum
  - Unlicensed spectrum is also getting crowded
  - Win buy Verizon in 700MHz auction means many feel white spaces are last chance
  - Users of licensed spectrum, like digital TV, unlikely to experiment in the same way
  - Biggest risk is question of interference
  - Testing is pending, both sides are pushing hard
  - Proponents want fixed uses and mobile devices

## Offset

## Topic

25:29

- The latter may be the most problematic for interference
- Article notes fixed uses could be a big win for rural broadband
- I'd like to see fixed use for broadband anywhere, as an abundant platform for competition
- Advocates for mobile probably looking to compete with licensed cell spectrum uses
- With issues plaguing test devices, may be increasing tensions
- Only live testing by the responsible agency, FCC, will answer both side's concerns
- New algorithm exploits symmetry
  - [http://www.eetimes.com/rss/showArticle.jhtml?articleID=208403608&cid=RSSfeed\\_eetimes\\_newsRSS](http://www.eetimes.com/rss/showArticle.jhtml?articleID=208403608&cid=RSSfeed_eetimes_newsRSS)
  - The algorithm is called "Saucy"
  - Based on University of Michigan research
  - Looking into problem of graph automorphism
  - Its application deals with automating design
  - Think using a program to automatically determine the shortest route on a network
  - The possible combinations are enormous, makes it cost prohibitive to calculate the absolute best
  - The new algorithm finds symmetries
  - In this case symmetry is defined as options that compute to the same outcome
  - This allows large sets of combinations to be discarded
  - Naturally can speed up a combinatorial search by effectively shrinking the space
  - State of research shows algorithm performs in seconds what the next best algorithm still takes considerable time to compute
  - Even helps with problems with no known solution
  - Article uses example of fitting ten pigeons in nine holes
  - Algorithm is smart enough to reduce this to a single calculation and determines there is no solution
  - Has wide applications as many problems are partially or wholly combinatorial problems

28:04

- Google preparing neutrality focused net analysis tools for typical user
  - [http://go.theregister.com/feed/www.theregister.co.uk/2008/06/13/google\\_network\\_management\\_tools/](http://go.theregister.com/feed/www.theregister.co.uk/2008/06/13/google_network_management_tools/)
  - The news came out of a panel at Santa Clara University
  - No release detail or details
  - Very clear that the tools will be for normal users
  - Google now also appears to quite strongly oppose operators working for tiered internet
  - Quotes from senior policy director Richard Whitt
  - Apparently, Google crunched the numbers
  - At one point figured it would do well enough in a tiered internet

## Offset

## Topic

- Google's decision to side with neutrality is framed as a move to favor innovation
- Recognizes their own success was thanks to an open, neutral network
- Whitt's co-panelists were George Ou, Richard Bennet
- Both experts at networking, also skeptical of regulation
- Others have promised, even delivered tools
- Most are for power users
- The tool from the network neutrality squad, started by Lauren Wienstein, was Windows only when I checked a few weeks ago
- Regardless of view, the promise to to start to reveal what is really going on
- The proof will be when the tools arrive, just accessible are they
- More importantly, what they really reveal
- Will there be a way to share findings?
- If that info is locked up on each user's system, may not be too useful after all

31:33

- **tail -f**

31:52

- Canadian DMCA to be revealed
  - <http://feeds.feedburner.com/~r/boingboing/iBag/~3/309893758/canadian-industry-mi-1.html>
  - Wrote on this extensively on the blog
  - <http://thecommandline.net/2008/06/12/first-details-on-canadian-bill-c-61/>
  - Bill was tabled, introduced formally, and is already being analyzed
  - Professor Michael Geist has said the most so far
  - <http://www.michaelgeist.ca/>
  - <http://thecommandline.net/2008/06/12/geist-on-canadian-dmca/>
  - <http://thecommandline.net/2008/06/13/more-from-geist-on-canadian-dmca/>
- Details on Canadian DMCA
  - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/310571655/20080612-canadian-dmca-brings-balanced-copyright-to-canada.html>
  - A good concise overview
  - Sheds some light on the same fine print Geist identifies
  - Consumer backup right limited to non-digital works
  - Circumvention of DRM is made illegal
  - Very few exceptions
  - No public discussion, like US DMCA, of other possible exceptions
- Canadian copyright comic book
  - <http://feeds.feedburner.com/~r/MichaelGeistsBlog/~3/309601030/>
  - Short work but very information dense
  - Built out of quotations, all linked

## Offset

## Topic

- Excellent example of remix art
- Plenty of links on the last page to opportunities to act
- Lots of things to consider on how Canada got to this point
- Geist made the point that Israel, NZ have face the pressure for normalization and preserved consumer rights successfully
- Anarchy and mass hysteria have not broken out in either of these countries

35:39

### • 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 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