

Offset	Topic
00:17	<ul style="list-style-type: none"> <li>• <b>Intro</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Balticon this coming weekend               <ul style="list-style-type: none"> <li>• No news show on 5/25</li> <li>• Was originally going to skip this week's feature</li> <li>• Lucked into an interview, will keep that as a surprise for Wednesday</li> </ul> </li> </ul>
02:35	<ul style="list-style-type: none"> <li>• <b>Security Alerts</b></li> </ul>
02:55	<ul style="list-style-type: none"> <li>• Debian fixes serious crypto bug               <ul style="list-style-type: none"> <li>• <a href="http://go.theregister.com/feed/www.theregister.co.uk/2008/05/13/debian_openssl_bug/">http://go.theregister.com/feed/www.theregister.co.uk/2008/05/13/debian_openssl_bug/</a></li> <li>• This is a bug in the pseudo random number generator</li> <li>• Results in predictable keys being generated for OpenSSL</li> <li>• In versions starting with 0.9.8c-1, as early as September 2006</li> <li>• Affects anything that uses OpenSSL for key generation, including SSH</li> <li>• Debian has issued a patch</li> <li>• Admins will need to regenerate keys after patching</li> <li>• Open questions whether this is a Debian specific problem</li> <li>• One investigator traced it to a Debian specific attempt to silence a debugger warning</li> <li>• Another suggests it may be a problem with OpenSSL itself, dating from May 2006</li> <li>• No confirmation of the latter as of yet</li> </ul> </li> </ul>
05:19	<ul style="list-style-type: none"> <li>• Secure PayPal page has been cracked               <ul style="list-style-type: none"> <li>• <a href="http://go.theregister.com/feed/www.theregister.co.uk/2008/05/16/paypal_page_succumbs_to_xss/">http://go.theregister.com/feed/www.theregister.co.uk/2008/05/16/paypal_page_succumbs_to_xss/</a></li> <li>• A serious scripting error has been discovered with PayPal</li> <li>• Could allow more convincing spoofs of their page</li> <li>• This despite using new SSL extensions</li> <li>• This is the feature that turns the address bar green in certain browsers</li> <li>• Finnish researcher Harry Sintonen was able to inject content into such a protected page</li> <li>• Doubly dangerous for those that put too much stock into the SSL extension</li> <li>• eBay has not addressed yet despite fairly comprehensive proof of concept</li> <li>• Article details several demonstrations that could steal a wide variety of data</li> <li>• PayPal has said they are looking into it, don't believe has been exploited yet</li> </ul> </li> </ul>

## Offset

## Topic

- This extended validation SSL was at the heart of PayPal saying they wouldn't support Safari
- More of a blanket statement about browser support for the extension
- Really shows there is no silver bullet, need to be actively securing on many fronts

08:02

### • News

08:16

- Providing the social aspect of the workplace for remote workers
  - <http://www.theglobeandmail.com/servlet/story/RTGAM.20080509.wgtbizsoftware0512/BNStory/Technology/?page=rss&id=RTGAM.20080509.wgtbizsoftware0512>
  - Researchers implicitly acknowledge value of social interaction
  - IBM working on new knowledge management system
    - At its core, similar to many such projects
    - Leavened with status updates like Facebook
    - Ability to post pictures, videos
    - Help add context to communications
  - Intel also experimenting
    - Started with virtual business cards, rich media in addition to standard info
    - Looking into virtual worlds, as well
  - Both companies are large, multinational, with off shored and remote workers
  - Article talks about virtual spaces filling in implicit communications
  - Make people feel embedded in space, presence of others
  - Some also trying to add pure social
  - IBM has an Inward Bounds, virtual gaming initiative
  - Also trying to capture ad hoc collaboration used to happen in hallways
  - Do identify risk of skewed politics
  - Introverts may be more outspoken in virtual spaces
  - May exacerbate generation gap
  - Benefits overall are still hard to quantify
  - Hints at reputation, trust which may net improved collaboration
  - Article is also skeptical that need for real meetings will ever be entirely replaced
  - I think there is real value, here
  - Modeling popular social apps probably not the best approach
  - Researching the social aspects and directly modeling will last better
  - The increasing phenomenon of hyper-connectivity
    - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/290161426/20080514-no-off-switch-hyperconnectivity-on-the-rise.html>
    - Study reveals a small but growing minority

## Offset

## Topic

13:48

- Coupled with other studies that show problems with multitasking and email stress, this is a trend to watch
- Do the efforts of companies to provide virtual connections have the potential to make this worse?
- USAF considers building its own botnet
  - <http://feeds.wired.com/~r/wired/topheadlines/~3/288873475/air-force-col-w.html>
  - I put this in the same class as a beneficial worm
  - Col. Charles W. Williamson III proposing build captive botnet
  - To use for DDoS attacks
  - Wrote up idea in Armed Forces Journal
  - Thankfully, not talking about infecting public at large
  - Would just install on non-classified government systems
  - Even restore junked computers to use for this purpose
  - Article correctly cites problems imposed on route nodes between attackers and target
  - Also implies resources better spent on more mature, sophisticated capabilities
  - Silly to build a botnet just because foes have one
  - How about further research of how to non-permanently disable infrastructure?
  - Law of unintended consequences seems to indicate a huge downside
  - Risks of sensitive systems inadvertently getting included
  - Exploitable vulnerabilities in nodes allowing someone else to subvert
  - That would allow a direct attack on the militaries internal network

17:06

- End of analog TV will bring increase in problems
  - <http://feeds.feedburner.com/~r/boingboing/iBag/~3/289531513/analog-switchoff-drm.html>
  - Opinion piece on TidBits
  - Author reflecting on entertainment options at hotel for CES
  - Mentions a digital TV education video from CEA
  - A loaded PSA for digital broadcast, trying to sell as free benefit to consumer
  - Sets up as foil to exploration of hidden dangers, issues
  - First is unwanted complexity
    - Converter boxes with 100 button remotes
    - Those most likely to keep old TVs least likely to be prepared to deal
  - No direct control schemes, yet, but the fact the HD digital is riddled predicts it is likely
    - Uses argument of format tax
    - Don't have to stretch to list out many options, all time limited, all priced arbitrarily

## Offset

## Topic

20:59

- All from existing digital formats
- Incentive to keep this going is too great for industry to go back
- Defeated the broadcast flag previously, but the potential reward for broadcasters almost guarantees it will return in some form
- Main thrust of opinion is that arbitrarily crippling technology is wrong
- Admits technologically savvy will not be burdened
- Vast minority, though
- Dovetails with the argument FSF advocates have been making through the DefectiveByDesign movement, site
- Trying to popularize the issues, invite commentary, discussion and action
- Highlight that those reader article need to think about the majority
- NBC activates broadcast flag
  - <http://arstechnica.com/news.ars/post/20080514-nbc-vista-copy-protection-snafu-reminds-us-why-drm-stinks.html>
  - This appears to only effect Vista Media Center Edition users
  - The flag was activated Monday night, during prime time
  - Included in over the air and cable broadcast
  - Microsoft, NBC looking into it
  - Similar to Tivo case last year or the year before
  - Claimed it was "accidental" though that seems unlikely
  - Tivo and DirecTV customers were unaffected
  - Serves as an unsettling reminder that content is increasingly not under our control
  - Outside of outright piracy, this is not right
  - Sony v. Universal established our right to time shift
  - This sort of overbearing control will have a blow back
  - Consumers don't like to be surprised
  - This is inconsistent with their use of the content, to date
- NBC flagging digital content
  - <http://www.eff.org/deeplinks/2008/05/update-nbc-and-microsoft>
  - Explains the EFF's fight against the broadcast flag
  - A fight they won
  - No manufacturer is required to enforce the flag although broadcasters are apparently still free to send it, part of the ATSC digital TV standard
  - That's the real kicker of this incident
  - Microsoft is not obligated to respect the flag
  - So why did they?
  - EFF is trying to figure out if it is a technical glitch, part of some other DRM scheme or just an accident

24:45

- **tail -f**

25:04

- Cases going against RIAA and reconsider Thomas case ruling

## Offset

## Topic

- <http://techdirt.com/articles/20080515/1228441125.shtml>
- Court has awarded Tanya Andersen \$108K in legal fees from RIAA
- This in response to the original suit
- After her being proven innocent
- Unrelated to her counter suit, trying to stop RIAA suits altogether
- Bigger news is in the Jammie Thomas case
- The ruling was against a binding precedent in the same circuit
- Judge is now admitting he may have made a severe error in jury instructions
- The jury instructions were altered at the behest of the RIAA
- Made to more closely match the RIAA's desired definition of making available as infringement
- May be possible judge will order a new trial
- Error of law may result in new trial for Jammie Thomas
  - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/291051629/20080515-jammie-thomas-likely-to-get-new-trial.html>
  - The problems is exactly because of the binding precedent
  - Unrelated to Thomas' appeal which is based on the size of the damages
  - Judge isn't addressing damages at all
  - A retrial will probably not go in Thomas' favor
  - However, it will erode the making available theory considerably

27:51

## • 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