

2007-01-21 Show Notes

Offset	Topic
00:17	<ul style="list-style-type: none">• Intro
	<ul style="list-style-type: none">• Listen for me on Speaking of Beer in the next Micro Brewed segment• Finished reading Theme Punks draft
03:04	<ul style="list-style-type: none">• Listener Feedback
	<ul style="list-style-type: none">• Discussion of Diamond Age on SciFi with Brian
04:34	<ul style="list-style-type: none">• Security Alerts
04:37	<ul style="list-style-type: none">• SHA-1 cracked<ul style="list-style-type: none">• http://rss.slashdot.org/~r/slashdot/eqWf/~3/78610270/article.pl• This is poor reporting• Digests are not encryption• MD5 and SHA1 are two separate things• Is accurate that this research first showed vulnerability in MD5 and other hashes• Vulnerability isn't reversing the hash, but being about to claim the digest is valid from a spoofed input• SHA-2 (224 through 512) may be vulnerable but not provably• Probably another NIST bake off in the works, or called for
08:56	<ul style="list-style-type: none">• News
09:20	<ul style="list-style-type: none">• Update on Cap'n Crunch, John Draper<ul style="list-style-type: none">• http://www.boingboing.net/2007/01/16/capn_crunch_at_63.html• Free version available http://online.wsj.com/public/article/SB116863379291775523-__EQCu93LyjSommsN6J7qiCozoo8_20070122.html?mod=blogs• An odd dichotomy, his daily life and still being an invited speaker• Besides his phreaking history, wrote one of the first word processors and technology for telephone menu systems• Article touches on "off-the-grid" community of hackers• Bartering work for goods, services is quite interesting• Sounds mildly autistic, definitely aspergic• Also a fascinating look back at the start of personal computing, when the community was small• Sounds like legal run ins in some ways limited his involvement with the PC boom• Did manage a "coporate career" from the seventies up to 1980• Some of his current woes seem to be circumstance, others seem self inflicted
14:09	<ul style="list-style-type: none">• FUSE comes to the Mac<ul style="list-style-type: none">• http://apple.slashdot.org/article.pl?sid=07/01/17/0257207&from=rss• Thanks to Amit Singh• File System in User Space

Offset

Topic

16:54

- Enables all kinds of need possibilities, like SSHFS
- Means even more interesting tools from Linux, BSD will run on the Mac with less fuss
- <http://www.downloadsquad.com/2007/01/17/secure-remote-disks-sshfs-for-mac-the-made-easy/>
- Cocoa front end for SSHFS and MacFUSE
- Is an Alpha release
- DLS gives some good tips and hints for use
- iPhone, Open Moko
 - iPhone crippleware claims
 - <http://feeds.macworld.com/~r/macworld/all/~3/76127096/index.php>
 - Another mainstream publication criticizing a new product for the inclusion of DRM
 - The point about the copy protection battles being over mirrors a point in Free Culture
 - The play list article is too defensive of Apple
 - The NYT article misses, perhaps, that the iPhone is identical to an iPod in this respect
 - I consider it crippled more because it is closed to 3rd party applications
 - Quiet open phone, Open Moko
 - http://go.theregister.com/feed/http://www.regdeveloper.co.uk/2007/01/15/open_phone/
 - Showed off at CES during the Macworld hullabaloo
 - Some hardware, GPRS, is more modest but it will improve if they continue to rev the device
 - Has several things over the iPhone, a MicroSD slot, full USB, both as device and host
 - Seem committed to open source as more than marketing
 - Trithemius will be getting one, I expect to talk about his experience getting it on a network
 - Open Moko schedule announced
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/78523768/article.pl>
 - Developer units ship March 11th
 - General availability still TBD

22:46

- Series of Tubes implemented
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/75770497/article.pl>
 - Windows only
 - Just another file sharing app
 - Tube sounds like a queue, trying to use the tube reference for some cache
 - Innovation seems more in the high level functionality, ease of use
 - This is only "compelling" to users who don't know any better

Offset	Topic
24:16	<ul style="list-style-type: none"> • tail -f
02:42	<ul style="list-style-type: none"> • AACS <ul style="list-style-type: none"> • AACS group responds <ul style="list-style-type: none"> • http://www.theglobeandmail.com/servlet/story/RTGAM.20070118.wdvsecurity0118/BNStory/Technology/?page=rss&id=RTGAM.20070118.wdvsecurity0118 • Involves Michael Ayers, who spoke at USC • For more info on the specifics of how they identified the breach and closed it, see Felten's site • Blu-ray version of AACS supposedly cracked <ul style="list-style-type: none"> • http://feeds.engadget.com/~r/weblogsinc/engadget/~3/78519403/ • Belies Ayers remarks about this not being a class break • Looks like some of the same techniques, and hence vulnerabilities, apply
27:27	<ul style="list-style-type: none"> • Vista DRM <ul style="list-style-type: none"> • Talked about this on 12/31/2006 • Security Now interviews Peter Guttman <ul style="list-style-type: none"> • http://feeds.feedburner.com/~r/boingboing/iBag/~3/75003760/vista_suicide_note_r.html • Responded to criticism that Hollywood won't release content unless DRM is implemented so heavy handedly • Belies that OEMs like DRM for their own reasons, lock in • Guttman mentions he is revising the paper • Discusses more detail about the paper and Microsoft's spec • Microsofts response to DRM critics <ul style="list-style-type: none"> • http://rss.slashdot.org/~r/slashdot/eqWf/~3/78734963/article.pl • "Better driver quality" makes me feel that Guttman was more right in his interpretation • This guys doesn't address the OEM criticism and I suspect they will be left holding the bag, like in the past • Still remains to be seen what the true burden will be
32:16	<ul style="list-style-type: none"> • Outro <ul style="list-style-type: none"> • Contact me <ul style="list-style-type: none"> • Email to feedback@thecommandline.net • Web site at http://thecommandline.net/ • IM to command.line@skype • Listener comment line is 360-252-7284 • del.icio.us tag is "for:cmdln" • I'd like to thank 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 <ul style="list-style-type: none"> • http://creativecommons.org/licenses/by-nc-sa/2.5/ • Attribution, non-commercial, share alike