

<u>Offset</u>	<u>Topic</u>
00:17	<ul style="list-style-type: none"> • Intro
	<ul style="list-style-type: none"> • Dragon*Con in a few days
03:32	<ul style="list-style-type: none"> • Security Alerts
03:51	<ul style="list-style-type: none"> • Clipboard hijacking attack
06:37	<ul style="list-style-type: none"> • http://news.bbc.co.uk/2/hi/technology/7567889.stm • The attack is Flash based • It puts a link in the user's clipboard • The link leads to a fake security site • The article describes the link as hard to delete • The attack endlessly re-writes the clipboard, replacing whatever the user places there • Affects Windows and Mac users using Firefox • Can be stopped by either killing the browser process or rebooting • Site at the link claims user's machine is riddled with malware • Clearly a scam to get folks to purchase a bogus product or to capture their personal details • Attack is not widespread but has shown up in a variety of spam • Curious about how this works if the page with the Flash is unloaded • Is this a fixable problem? • Further, using an extension like NoScript will protect you • Blocks flash by default
06:37	<ul style="list-style-type: none"> • New crypto attack from Adi Shamir <ul style="list-style-type: none"> • http://www.schneier.com/blog/archives/2008/08/adi_shamirs_cub.html • This is new research from Adi Shamir, the S in RSA • Attack is applicable to a wide variety of the math underpinning crypto • Not just ciphers but also hash functions • Bruce adds further edits that certain algorithms are not susceptible • It seems like if the math in question has a high degree polynomial, it is resistant • This explicitly rules out AES • Also rules out newer block ciphers like DES, Blowfish and Twofish • More on the research after it is published • Reinforces that no math is bullet proof • Given enough time, enough minds, flaws will be found, exposed • Similar to much more aggressive attacks on hash functions, like MD5 and SHA1
09:58	<ul style="list-style-type: none"> • News
10:12	<ul style="list-style-type: none"> • Questions about cloud computing begged by Google outages

- http://www.infoworld.com/article/08/08/15/Google_Apps_admins_jittery_about_Gmail_hopeful_about_future-IDGNS_1.html
- Google had a couple of outages this past week
- Article details the impacts on some customers
- Begs the question of how this will affect the adoption of cloud computing
- The article mentions admins using forums, doing trouble shooting
- Are there more opportunities to better handle disaster and recovery in the cloud?
- Points out a serious downside
 - Don't have to worry about hardware, software operations
 - Lose some visibility that might help predict a problem
- Other than the scale, is it that much different than a corporate server losing a disk array or other failure?
- Frustrating because there is little an admin can do directly to recover
- A two hour turn around is not bad, though
- A local admin could re-purpose a spare system to handle 1 organizations email or applications, though
- Many in the article had the capability to run their own systems
- Some talked about using Google as a backup if outages persist
- Google puts all apps in a large bucket
- There may be some compartmentalization
- Other providers, ones that more clearly expose individual VMs may provide better risk management
- Smaller players may have less of a choice
- One admin in the article said they might leave Apps, stay away for a few years if outages persist
- If competitors are more resilient to outages, that could really hurt the risk averse
- Google, others could provide recovery options as part of the service
- May already do
- But see a real use for Google's appliance, a local node that can keep running minimum services if the cloud instances have trouble
- Increasingly, providers will have to address these and other risks that are effected by the nature of cloud computing
- New visual search engine for finding infringing uses
 - <http://arstechnica.com/news.ars/post/20080819-tineye-image-search-helps-ferret-out-copyright-riporoffs.html>
 - Service is called TinEye
 - Requires that you have the image already
 - This appears to be a hash based search
 - Article does note it can find matches that have been cropped and even minimally altered

Offset

Topic

19:33

- Quote from FAQ makes it sound like it yields similar results as well as exact matches
- Article initially focuses in on use to protect rights
- How about also using it to find rights holder to seek permission, give attribution?
- Ars tried the search engine, their results are worth the read
- Service requires registration
- Despite quote, results seem biased towards exact match
- Author new where one test photo had been used widely
 - TinEye find a very small number of hits
 - CEO explains this as a consequence of a small index as of yet
- CEO admits the usage to find a rights holder
- Offers additional reasons, such as try to uncover names, info in an unknown photo
- Still not necessarily for casual use
- Reminds me, though, of a complaint by Alex Curtis of PK about the orphan works problem
- In the absence of a registration database, a private search engine could do
 - A few years ago, there was none
 - Hopefully TinEye can succeed and fulfill this need
- Judge rules fair use should be consider before sending DMCA take downs
 - <http://www.eff.org/deeplinks/2008/08/judge-rules-content-owners-must-consider-fair-use->
 - This is the so-called dancing baby case, Lenz v. Universal
 - Plaintiff had posted a 29 second video of a toddler dancing
 - In the background, a Prince song was playing
 - Universal sent a DMCA takedown
 - Plaintiff found out when YouTube informed her they had taken down the video
 - Lenz sued for misrepresentation under the DMCA, arguing fair use
 - Universal of course file a motion to dismiss
 - Judge Fogel agreed with plaintiff
 - Basically stated that fair use must be part of a consideration of a DMCA violation
 - Universal argued this was not possible
 - Judge stated that section 512c already requires a review before sending a notice
 - Stated that a fair use consideration as part of that review is not too much of a stretch
 - Fogel also sees this as necessary to help prevent abuse
 - This was heard in a federal court, neither of the EFF articles say which

Offset

Topic

22:13

- Hopefully it helps urge some sanity in other cases of DMCA takedowns
- If Universal appeals, could be an even bigger win if a higher court judge agrees with Fogel
- Was standardizing on JavaScript a mistake?
 - http://weblog.infoworld.com/fatalexception/archives/2008/08/was_javascript.html
 - Neil McAllister, Fatal Exception blog, responds to Harmony project
 - Quotes Adobe stake holder in ECMAscript 4
 - Echoes my concerns about web applications of scale
 - McAllister is skeptical that better standards would help in all cases
 - Thinks smaller applications just as likely to be as ad hoc as always
 - Generalizes to suggest that a single language, especially designed by committee, is a bad idea
 - Cites Ada by way of example, that folks fled to C to escape restrictions of Ada
 - Suggests that we take a page from the MVC pattern
 - Thinks the current approach welds the control logic to closely with the view, the browser
 - Highlights the stigma of old approaches, browser plugins
 - Thinks we've moved past this, that Google Gears for one is well received
 - Also explains it provides some general facilities many web application can use
 - Wonders if the stigma against plugins is still valid?
 - More users have access to broadband instead of dial up
 - I don't think the security issues have progressed much, though
 - A small number of plugins could be useful in the way he suggests
 - Opening things up too much, though, could lead to many headaches
 - Critics of FireFox cite that with too many extensions, the browser bogs, becomes unstable
 - Why not develop something like CPAN for JavaScript compatible modules
 - Design an API for extensions in other languages
 - Doesn't have to be done by committee, which is part of his point
 - I do agree with his final point, that a killer app will be the best driver to adopt this approach
 - So what might be better is JavaScript as a default and a standard way for a page author to hook some other language, technology
 - We already have some of the pieces like the language attribute of the script tag
 - Need to make security better, distribution easier

28:55

- `tail -f`

29:14

- Elektra v. Barker case is settled
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/368363297/article.pl>

31:05

- This case was notable for the RIAA's use of its making available argument
- Barker put forward some interesting active defenses
- Questions about size of penalties, investigatory practices
- None of that will be tested in a court, now
- No reason I can find for why they settled
- The settlement is for a bit over \$6K, paid \$110 a time
- Probably a money issue
- Surprising given the judge's reversal on making available in the Thomas case
- Also surprising given Tanya Andersen's victory
- Victory for MIT students against MBTA
 - <http://www.eff.org/deeplinks/2008/08/victory-mit-students-mbta-lawsuit-hearing>
 - Judge O'Toole lifted the injunction on the 19th
 - Did so on the basis that the MBTA is unlikely to prevail on the merits of the case
 - Judge decided the computer fraud and abuse act does not in fact govern security researchers talking to people
 - Judge punts in 1st Amendment question with MBTA v. MIT students
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/369481550/20080819-judge-lifts-gag-order-punts-on-first-amendment.html>
 - Judge did not rule on the free speech concerns raised by the EFF
 - The case will still go forward
 - MBTA may appeal the ruling, trying to restore the gag order
 - Students don't have any plans at this time to discuss their research now that they can
 - MBTA admits tickets are not secure
 - http://www.boston.com/news/local/articles/2008/08/20/mbta_admits_ticket_not_secure/
 - Looks like the admission came as part of O'Toole's hearing
 - Was probably key to him ruling against the proposed merits of the MBTA's case
 - Lawyers for the MBTA say they will now work with the students
 - I am skeptical, they said that before seeking the original injunction
 - MBTA is trying to represent this as a win
 - Claim the research only affects the paper ticket
 - Students disagree, citing issues with the RFID cards as well
 - MBTA claims it is already implementing changes to address what they think are limited problems
 - Also seem to think stopping the Defcon presentation was sufficient
 - Students still claim they wish to cooperate

Offset

Topic

- Based on my reading last week, seems like that was their attitude throughout
- Interview with MIT student hacker, Zack Anderson
 - <http://www.popularmechanics.com/technology/industry/4278892.html>
 - A more personal recitation
 - Covers what has been already discussed
 - Reinforces that Anderson, others, were willing to cooperate all throughout
 - Were not trying to cause trouble
 - Also re-iterates that their analysis was broad, not just the ticket technology itself

35:01

• **Outro**

- Contact me
 - Email to feedback@thecommandline.net
 - Web site at <http://thecommandline.net/>
 - IM to 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 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