

Offset	Topic
00:17	<ul style="list-style-type: none"> <li>• <b>Intro</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Closure on Reiser case <ul style="list-style-type: none"> <li>• What did the reporting leave out?</li> <li>• What if he had revealed the location of the body earlier on?</li> <li>• The fact that he knew that changes the geek defense</li> </ul> </li> </ul>
05:18	<ul style="list-style-type: none"> <li>• <b>Security Alerts</b></li> </ul>
05:38	<ul style="list-style-type: none"> <li>• Big reveal of DNS flaw <ul style="list-style-type: none"> <li>• <a href="http://go.theregister.com/feed/www.theregister.co.uk/2008/08/06/kaminsky_black_hat/">http://go.theregister.com/feed/www.theregister.co.uk/2008/08/06/kaminsky_black_hat/</a></li> <li>• The problem stems from a limit in a safety measure</li> <li>• DNS requests contain a random token</li> <li>• The tokens are 16 bit, though, meaning they max at 65K or so</li> <li>• A brute force attack can overcome these tokens because of the limited number</li> <li>• His talk has apparently convinced many skeptics of the real danger</li> <li>• Kaminsky also speculated on the variety of exploits the vulnerability made possible</li> <li>• <a href="http://voices.washingtonpost.com/securityfix/2008/08/kaminsky_details_dns_flaw_at_b.html">http://voices.washingtonpost.com/securityfix/2008/08/kaminsky_details_dns_flaw_at_b.html</a></li> <li>• More details on the attack scenarios described in the talk</li> <li>• Regression vulnerability in DNS patch <ul style="list-style-type: none"> <li>• <a href="http://www.nytimes.com/2008/08/09/technology/09flaw.html?_r=1&amp;hp&amp;oref=slogin">http://www.nytimes.com/2008/08/09/technology/09flaw.html?_r=1&amp;hp&amp;oref=slogin</a></li> <li>• Written up by a physicist, Evgeniy Polyakov</li> <li>• Claims he can reliably cause an invalid return for a DNS query</li> <li>• Other critics think the fix for the cache poisoning is just a band aid</li> <li>• The attack was conducted against BIND</li> <li>• This according to author's own blog</li> <li>• Don't know if it applies to other implementations</li> </ul> </li> </ul> </li> </ul>
09:10	<ul style="list-style-type: none"> <li>• Hackers kicked out of Black Hat for hacking <ul style="list-style-type: none"> <li>• <a href="http://blog.wired.com/27bstroke6/2008/08/french-reporter.html">http://blog.wired.com/27bstroke6/2008/08/french-reporter.html</a></li> <li>• Three french reporters were sniffing logins on the press network</li> <li>• Tried to convince organizers to post on Wall of Sheep</li> <li>• This is a shame based display, started at DefCon</li> <li>• Started running it at Black Hat for the first time this year</li> <li>• Wall of Sheep sniffs general conference network for non-secure login data</li> <li>• Press network is supposed to be off limits, though</li> <li>• Wall of Sheep is legal because attendees are notified</li> </ul> </li> </ul>

## Offset

## Topic

- Reporters actions are technically illegal since they monitored the private network unbeknownst to its users
- Press network private to wall them off from the free for all that occurs on regular network
- Three reports were from a media sponsor, had covered the conference before
- Apparently were honest about what they had done, don't appear to be malicious per se
- Still, for violating the rules, were ejected from the conference

11:42

### • News

11:57

- A software solution to bad hard drives
  - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/354985871/article.pl>
  - Author, Thanassis Tsiodras, concerned about problem of media failure
  - Even with a robust backup strategy, using same fallible media
  - Points out residual problems with other strategies from RAID to revision control
  - Suggests using error correcting codes, like Reed-Solomon
  - Store additional data, a checksum or error check value
  - With his scheme, need 16 errors in a smallish block to destroy the block
  - Describes some clever data layout based on physical sectors on disk
  - This interleaving of protected blocks means hitting that 16 error limit is very unlikely
  - Hacked some existing code
  - rsbep utility on Debian, part of the dvbackup software
    - dvbackup lets you use your DV based camcorder as a backup device
    - rsbep is the error correction utility for the package
  - Offers sources, including assembly for x86
  - Describes what he changed on rsbep and why
  - Has a screenshot of using the tool, very compelling
  - Need to bundle up files of interest, as a tar or similar file
  - Then use utility to create protected version
  - When restoring, adds an extra step, undoing the shield to be able to open restored file
  - Author claims this utility has saved his data repeatedly
  - Are there file systems that use this?
  - Could someone use this idea to write one or a module for FUSE?
  - Rather than building a UI, is it worth just making it transparent?
  - Portable C version built just fine on my OS X box
  - Simple test worked fine

## Offset

18:55

## Topic

- Need to think about how to incorporate this into critical backup needs
- HEA finalized in both House, Senate
  - <http://www.eff.org/deeplinks/2008/08/congress-bows-big-content-scapegoats-higher-ed>
  - This is a large package of reforms
  - Buried in it is a very contentious provision about policing infringing materials
  - Stipulates that universities must use technological deterrents
    - Traffic shaping and monitoring
    - Content filtering
  - Universities must also promote legal alternatives
  - ACM, others have identified these technologies as often not working and always increasing cost for universities to operate
  - Students don't care for DRM in legal alternatives, adopting to date has been poor even when free to students
  - Based on flawed assumptions
    - That universities have a higher rate of piracy
    - That their network managers are not already dealing with the issue
  - Universities hardly differ from the average, MPAA copped to flawed study data last year
  - Network managers do more than typical ISP, including user education and active punishment for proven offenders
  - Bills still needs to pass
  - Time to act
  - EFF is recommending voluntary collective licenses as an alternative
  - Universities pay a blanket license fee
  - Students get unrestricted access but artists still get compensated

22:47

- EFF educating, protecting hackers at Black Hat
  - <http://www.eff.org/press/archives/2008/08/05-0>
  - EFF has started a new project, Coders' Rights Project
  - As part of the launch, they provided access to a staff attorney
  - To answer questions about reverse engineering, vulnerability reporting, copyright, etc.
  - Meant to help ease researchers concerns from bogus legal threats
  - Continues their work against the provisions of the DMCA that act to restrict legitimate research
    - Think about the security implications of the Sony rootkit
    - Also some claims of DMCA violation on e-voting systems
  - Will expand the scope of their work under this project to computer crimes acts
  - Looking to narrow the scope of these laws
  - Also looking at tackle some issues with EULAs

## Offset

26:14

## Topic

- EFF doesn't clarify but I will, this is not just a legal defense fund
- Specifically for legitimate research
- The project page collects a lot of education material
- Also press releases and relevant news stories
- Two FAQs prominently placed, for reverse engineering, vulnerability research
- Ubiquitous data in the cloud
  - <http://arstechnica.com/news.ars/post/20080806-stateless-computing-the-future-of-the-cloud.html>
  - A presentation by Merrill Lynch's CTO, Jeffrey Birnbaum, at LinuxWorld
  - Uses the term stateless in a new way
  - What he means is a ubiquitous file system
  - Thinks part of the key to scaling cloud computing is accessing through this FS
  - Stateless seems to refer to lacking local state
  - Posits this will lead to a decoupling of software, data from physical machines
  - Like other cloud computing advocates, envisions discussing applications in terms of abstracted units of computation
  - Thinks this will ease deployment issues
  - Not so sure of that, think you need standards on VMs and cloning like Joyent post discussed
  - Specifically discusses regional mirroring and caching for network wide storage
  - ML has already partially implemented
  - Sounds like the applications in question are not just web applications
  - Sounds like some of what they are doing is traditional client and server apps
  - That's what I take away from his discussion of problems with Windows
  - Specifically that they use RDP to solve Windows not working well with network file systems, like NFS under Linux
  - Sees much of ML's hardware going underutilized
  - Early goal for their own plans is to see better utilization by being able to run any apps on any available hardware
  - Their focus is on the technology to place work on hardware
  - Obviously if they are successful means they can be cheaper hardware but more of it, especially as needed
  - Reminds me a bit of a recent article in CACM on Google's Map/Reduce
  - Much of what makes that work is the task coordination across the cloud, as much as the separation of mapping and reducing tasks
  - Birnbaum's talk matches trends I am seeing discussed in more places

Offset	Topic
31:33	<ul style="list-style-type: none"> <li>• That a traditional player like ML is adopting says something about the staying power of these trends</li> </ul>
31:52	<ul style="list-style-type: none"> <li>• <b>tail -f</b></li> <li>• Thomas trial may end in mistrial, retrial <ul style="list-style-type: none"> <li>• <a href="http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/356491442/20080805-judge-in-jammie-thomas-p2p-case-sounds-open-to-retrial.html">http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/356491442/20080805-judge-in-jammie-thomas-p2p-case-sounds-open-to-retrial.html</a></li> <li>• Judge Davis' hearing was this week</li> <li>• RIAA made same arguments about difficulties to prove infringement</li> <li>• Judge remained opposed to their interpretation</li> <li>• Observers think Davis was inclined towards granting a re-trial</li> <li>• RIAA seemed confident it could produce the require evidence it didn't submit in the original trial</li> <li>• Defense attorney work to have "authorized" downloads by RIAA investigators excluded</li> <li>• Judge's ruling to appear in another month or so</li> <li>• This is turning into anything but the slam dunk case the RIAA must have thought</li> <li>• Irony is if they hadn't fought so hard over the making available argument, then they'd only be having standard appeal instead of mistrial</li> </ul> </li> </ul>
33:57	<ul style="list-style-type: none"> <li>• Blizzard seeking to block opening of Glider sources <ul style="list-style-type: none"> <li>• <a href="http://virtuallyblind.com/2008/07/29/blizzard-seeks-permanent-injunction/">http://virtuallyblind.com/2008/07/29/blizzard-seeks-permanent-injunction/</a></li> <li>• After winning summary judgement, seeking permanent injunction</li> <li>• Wants to keep Glider off its servers, which makes sense</li> <li>• Also trying wants injunction against MDY releases sources</li> <li>• It is an unusual injunction to seek, though their reasoning makes a certain sort of sense</li> <li>• This is likely to be fought much more strenuously</li> <li>• The implications of the summary judgement are bad enough</li> <li>• Erosion of first sale doctrine as applies to software</li> <li>• But establishing precedent for preventing open source sharing</li> <li>• Scary thing is it may be granted</li> <li>• The summary judgement was on a copyright basis, not license or contract</li> <li>• Same judge may see open source release as further copyright infringement or inducement to infringe</li> <li>• Programmer developed on their own, without any proprietary knowledge</li> <li>• Shouldn't it fall under reverse engineering protections?</li> </ul> </li> </ul>
	<ul style="list-style-type: none"> <li>• <b>Outro</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Contact me <ul style="list-style-type: none"> <li>• Email to <a href="mailto:feedback@thecommandline.net">feedback@thecommandline.net</a></li> </ul> </li> </ul>

## Offset

## Topic

- 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