

Offset	Topic
00:17	<ul style="list-style-type: none"> <li>• <b>Intro</b></li> </ul>
	<ul style="list-style-type: none"> <li>• Review of Settlers of Catan</li> </ul>
04:39	<ul style="list-style-type: none"> <li>• <b>Security Alerts</b></li> </ul>
04:59	<ul style="list-style-type: none"> <li>• DNS vulnerability leaked then pulled <ul style="list-style-type: none"> <li>• <a href="http://rss.slashdot.org/~r/slashdot/eqWf/~3/341985322/article.pl">http://rss.slashdot.org/~r/slashdot/eqWf/~3/341985322/article.pl</a></li> <li>• Kaminsky had agreed to defer publication to allow coordinated updates</li> <li>• A reverse engineering expert, Halver Flake was musing about it</li> <li>• Apparently prompted someone who know the flaw to post details</li> <li>• Was quickly pulled though some cache copies can still be found</li> <li>• Interview with Kaminsky on DNS exploit <ul style="list-style-type: none"> <li>• <a href="http://blog.wired.com/27bstroke6/2008/07/kaminsky-on-how.html">http://blog.wired.com/27bstroke6/2008/07/kaminsky-on-how.html</a></li> <li>• More details about how the problem was discovered</li> <li>• Also how experts were pulled together to discuss how to address</li> <li>• Kaminsky prefers to be constructive about the leak</li> <li>• Had about a week and a half with the patch available before the leak</li> <li>• Also vendors were largely positively, willing to just get to work</li> <li>• Static has come more from security industry, pundits not those responsible for evaluating, producing patches</li> </ul> </li> </ul> </li> <li>• DNS flaw points out problems with discovery, patching <ul style="list-style-type: none"> <li>• <a href="http://feeds.wired.com/~r/wired/topheadlines/~3/344036307/securitymatters_0723">http://feeds.wired.com/~r/wired/topheadlines/~3/344036307/securitymatters_0723</a></li> <li>• Schneier sees this as evidence of need for a more profound change</li> <li>• Has been extolling building in security at the design even before implementing</li> <li>• Re-iterates how that would have helped here</li> <li>• Points out how including a security engineer in projects would be more cost effective than patching after the fact</li> <li>• I think this is even more of a benefit</li> <li>• Even if we reduce the patch treadmill as he calls it I doubt it will ever go away</li> <li>• Having a security stakeholder as part of software all along could speed up evaluating flaw info, patches and the like</li> <li>• Could make designs easier to modify to incorporate new information</li> </ul> </li> <li>• DNS attack code published <ul style="list-style-type: none"> <li>• <a href="http://arstechnica.com/news.ars/post/20080726-new-dns-exploit-now-in-the-wild-and-having-a-blast.html">http://arstechnica.com/news.ars/post/20080726-new-dns-exploit-now-in-the-wild-and-having-a-blast.html</a></li> <li>• Exploit is a Metasploit module</li> </ul> </li> </ul>

## Offset

## Topic

- The attack involves target upstream DNS servers
- Takes advantage of the recursive nature of DNS
- If any server cannot find a name, it looks upstream
- Currently implementation of that recursive search is too trusting
- At the two week mark, patch deployment was estimated at 52%
- Live exploit should accelerate uptake of the patch
- ISPs dragging feet on DNS patches
  - [http://go.theregister.com/feed/www.theregister.co.uk/2008/07/25/isps\\_slow\\_to\\_patch/](http://go.theregister.com/feed/www.theregister.co.uk/2008/07/25/isps_slow_to_patch/)
  - Surprising how many large ISPs have not patched yet
  - Article contains a link to Kaminsky's site where he has a test
  - Can determine if your ISP has patched and is safe
  - If your has not patched, you can use a secure alternative
  - Register recommends OpenDNS, I concur
  - In running the test myself, realized that those with home routers will want to update, as well
  - Got a warning that my router may need a patch, too

14:05

### • News

14:19

- Open cloud computing
  - <http://cloudcomputing.sys-con.com/read/613436.htm>
  - Mike Linksvayer sent a link in response to my mention of Autonmo.us on the site
  - <http://lists.canonical.org/pipermail/kragen-tol/2006-July/000818.html>
  - This really makes the group's focus clear
  - Not about users but about applications
  - Being able to pick your own provider and move incidentally achieves data portability
  - In short, applying open source principles to cloud computing
  - Encountered another article on open cloud computing
  - Written by David Young, at Joyent
  - Joyent is his first cloud computing endeavor
  - Company does some well positioned
  - Offers application hosting as well as basic office, collaboration web applications
  - Starts by discussing the definition of cloud computing
  - Joyent even did a brief industry survey that he links to
  - Mentions SaaS and PaaS but really can be simply opposed to edge of network applications
  - In the absence of a firm definition, even a de facto on, starts to speculate on what clouds should be
  - Starting assumption i they should be open
  - Then lists nine items to accomplish a truly open cloud

## Offset

## Topic

20:21

- Need to be able to self-serve compute nodes, including creating new ones, moving them and automated/transparent recovering
- Talks about state layer interoperability
- Mentions BigTable and SimpleDB but is really talking about a common API/protocol for data storage
- Implementable by anyone, scalable without impacting applications that use
- Use SQL or a SQL-like language to interface so application developers can just think of it as a database
- Measures his own services against these criteria, not surprisingly does well
- Hints at future development
- I like the idea of delegating scalability to a provider but not totally sacrificing control, ease of development, deployment
- MPAA interviewed on petition to allow SOC
  - <http://arstechnica.com/news.ars/post/20080720-mpaa-dvr-blocking-about-multibillion-dollar-theft-problem.html>
  - Haven't talked about SOC before
  - FCC currently restricts broadcasters from using broadcast flags or SOC
  - Selectable output control means broadcaster could forbid different types of outputs
  - DVI, HDMI, component, etc.
  - MPAA has made a plea on behalf of studios to waive restriction
  - They say the waiver is needed for new on-demand business models
  - Offer new movies between theatrical and disc release
  - Want to forestall piracy of this new business model, so as not to erode disc sales
  - Critics find the plea vague
    - Doesn't accept or admit any limitations on use
    - Doesn't clearly defined which devices would be affected and which exempted
  - Again, seems to be about controlling, preventing innovation by others
  - MPAA wanted to clarify with Ars, claim it is not about blocking home recording
  - Discussion didn't seem to clear anything up
  - MPAA insists this is not about stopping recording
  - Preventing output on high quality protocols, though, seems to be about stopping production of high quality copies
  - MPAA folks just kept re-iterating new business model, getting content sooner
  - Doesn't change that the plea is just too vague as to how studios will use the waiver if they get it
  - AT&T, DirecTV support MPAA's SOC play

## Offset

## Topic

27:58

- <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/343167711/20080722-att-directv-back-mpaas-dvr-blocking-initiative.html>
- Initial comments conclude
- About twenty parties weighed in
- A mix of supporters and critics
- AT&T and DirecTV don't think it would hurt current consumer choice
- Without clear limits in the plea, though, the studios certainly could limit existing programming as well as new
- That is the core of the critics comments
- National Theater Owners and Independent Film and Television Association also amongst critics
- Probably feel it will hurt their current business practices
- Some are in the middle, willing to support but with conditions, restrictions
- More info from PK on MPAA and SOC
  - <http://feeds.publicknowledge.org/~r/publicknowledge-fulltext/~3/342928544/1668>
  - Sums up PK's stance well
  - Written by Jef Pearlman who was a techie before a lawyer
  - Clear summation of the issues, accessible
- USPTO to invalidate many, most software patents
  - <http://www.patentlyo.com/patent/2008/07/the-death-of-go.html>
  - PTO seems to be revising its standards
  - Based on three cases challenging section 101
  - Seems to be moving towards requiring clear physical transformation as being patentable
  - Or if it is tied to a particular machine
  - Article interpretation is that a general purpose computer is not a particular machine
  - Thinks that means we could see a large swath of software patents invalidated
  - Article considers a couple of specific cases, including Google's PageRank algorithm
  - Thinks creativity, innovation will be trumped by their interpretation of the PTO's emerging standard
  - More information on changes at USPTO
    - <http://www.groklaw.net/article.php?story=20080724202700686>
    - Clarifies the author, Duffy, has filed a brief in one of the key cases
    - Speculates the article is a bit of advocacy
    - Meant to sway a judge's opinion, may not be a genuine speculation
    - Offers a contrasting opinion from another lawyer
    - Even the blog owner of Patently O disagrees with the author

<u>Offset</u>	<u>Topic</u>
30:45	<ul style="list-style-type: none"> <li>• Also questions Duffy's conclusion that elimination of software patents would disrupt innovation industry</li> <li>• Cites views, research in line with anti-patent advocates who think the opposite is true</li> <li>• New foundation to support open web standards efforts <ul style="list-style-type: none"> <li>• <a href="http://www.webmonkey.com/blog/New_Foundation_Wants_to_Bridge_the_Gaps_Between_Open_Web_Tools">http://www.webmonkey.com/blog/New_Foundation_Wants_to_Bridge_the_Gaps_Between_Open_Web_Tools</a></li> <li>• Announced by Six Apart's David Recordon, at OSCON</li> <li>• <a href="http://openwebfoundation.org/2008/07/announcing-the-open-web-foundation.html">http://openwebfoundation.org/2008/07/announcing-the-open-web-foundation.html</a></li> <li>• Appears to be modeled after the Apache Foundation</li> <li>• Will provide legal support for open standards, like OAuth and OpenID</li> <li>• Meant to help answer questions potential corporate adopters may have</li> <li>• Mostly questions about liabilities, exposures like patents, privacy, etc.</li> <li>• If successful, should make open standards more attractive</li> <li>• Also provide a place for those working on standards, specifications to meet and coordinate efforts</li> <li>• Not much other detail though they have a community site, forum set up for discussion</li> <li>• Founders think it is complementary to Autonomo.us</li> <li>• OWF to concentrate on adoption, other to focus more perhaps on how standards, specs ensure user freedom</li> <li>• For instance, recent post on Autonomo.us site is about Jesse Vincent's Prophet</li> <li>• This is an open source, distributed state layer or data store</li> <li>• Autonomo.us is highlighting specific efforts, principles, not just standards</li> <li>• OWF more open openness for interoperability</li> <li>• Why not W3c or IETF? <ul style="list-style-type: none"> <li>• <a href="http://www.links.org/?p=351">http://www.links.org/?p=351</a></li> <li>• Discusses organizational differences</li> <li>• Limitations of W3C and IETF that OWF is looking to avoid</li> <li>• Clearly re-inforces focus on developing, advocating standards</li> </ul> </li> </ul> </li> </ul>
34:33	<ul style="list-style-type: none"> <li>• <code>tail -f</code></li> </ul>
34:52	<ul style="list-style-type: none"> <li>• Code released for cold boot encryption attack <ul style="list-style-type: none"> <li>• <a href="http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/342170246/20080721-source-code-published-for-cold-boot-exploit.html">http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/342170246/20080721-source-code-published-for-cold-boot-exploit.html</a></li> <li>• Based on researcher by Ed Felten at Princeton and others</li> <li>• Originally released back in February</li> <li>• Code is released from the same researchers</li> </ul> </li> </ul>

## Offset

## Topic

35:44

- Will hopefully spur vendors to try to come up with practical solutions
- Slower than hoped adoption of OpenID
  - [http://feeds.wired.com/~r/wired/topheadlines/~3/341891010/Dear\\_Open\\_ID%3A\\_You\\_Deserve\\_Better](http://feeds.wired.com/~r/wired/topheadlines/~3/341891010/Dear_Open_ID%3A_You_Deserve_Better)
  - Itemizes some of the problems with adoption
  - Much of the support is one way
  - Big adopters allow their accounts to be used as OpenIDs
  - Do not let folks use other OpenIDs to log into them, like Yahoo!
  - Adopters aren't using all of what is available
  - Aren't re-using identity data
  - Forcing users to re-register which defeats much of the point
  - Points out next stages for adoption, improvement
  - Is a cute reminder to big services not to rest on laurels

37:16

### • **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