

2008-02-10 Show Notes

Offset	Topic
00:17	<ul style="list-style-type: none">• Intro
	<ul style="list-style-type: none">• Farpoint coming up, 2/15-17<ul style="list-style-type: none">• Will be reprising my copyright, creative commons, legal issues panel• Will be working with the video folks to show some relevant material• May also show some or all of Steal This Film• Mid-Atlantic Podcasters Roundtable Saturday 10:00 AM• Intellectual Property - The Oil of the 21st Century Saturday 3:00 PM• All The News That's Fit Not to Print Sunday 12:00 AM• What's on Your Mind? Blogging, Audio Blogging and Podcasts Sunday 3:00 PM
04:06	<ul style="list-style-type: none">• Listener Feedback
	<ul style="list-style-type: none">• Jed on AOP<ul style="list-style-type: none">• Thinking of it as a pre-compiler, macro language• Logging for debugging
06:39	<ul style="list-style-type: none">• Security Alerts
06:58	<ul style="list-style-type: none">• Antivirus inventor questions security best practices<ul style="list-style-type: none">• http://rss.slashdot.org/~r/slashdot/eqWf/~3/231094886/article.pl• Peter Tippet, chief scientist at ICSA and inventor of what became NAV• Presentation at computer forensics show• Says one third of practices are based on outdated information• Thinks time is wasted on vulnerabilities unlikely to be exploited• Takes disclosure, vulnerability and patch management to task in particular• Problem with that is his analogy is limited by laws of physics• Many rare exploits are only rare because of attacker inattention• Cost to fix may be higher than he'd like, but not the same as fixing a physical safety defect• The exercise of asking, though, is worthwhile• Automation can and does reduce cost of patch management, my favorite the auto update channel/feature• His criticism seems to be more on the research, knowledge management side• Acknowledges that resources are limited, need to be best prioritized• His sole point seems to boil down to that, best security dividend for investment, like security awareness training for employees
10:51	<ul style="list-style-type: none">• Firefox update includes ten security fixes<ul style="list-style-type: none">• http://go.theregister.com/feed/www.theregister.co.uk/2008/02/08/firefox_update/• Top three most critical fixes

Offset

Topic

- History browsing disclosure
- Privilege escalation that could be used by CSS attacks
- A memory corruption bug
- Also includes fix directory traversal via chrome handling, previously discussed here
- Available through built-in update mechanism
- Already vulnerable
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/232385359/article.pl>
 - Another directory traversal
 - Also appears to be exposed via protocol handling
 - This time through resource handler
 - Author suggests it is due to an incomplete fix of the chrome protocol handler
 - This is a risk of all such expedited fixes, that they are incomplete
 - Author has posted a proof of concept
 - NoScript will stop this exploit, too

13:59

• News

14:13

- Issues with Internet voting
 - <http://feeds.freedom-to-tinker.com/~r/freedom-to-tinker/~3/229012933/>
 - Internet voting arises more and more
 - This past week was primary vote, Super Tuesday
 - Libertarian part of AZ is conducting its entire vote online
 - Democratic parting experimenting with overseas voting
 - Military experimented with SERVE but was roundly criticized
 - SERVE was abandoned
 - Some EU states also experimenting
 - Good anecdote about friend from Estonia
 - Estonian system allows for vote overriding
 - Helps address voter coercion
 - Voter confidentiality/coercion, security bigger concerns
 - Libertarian system doesn't even use SSL
 - Dan Wallach didn't experiment far enough to find if allowed vote overriding
 - Democrats fair little better
 - Use SSL but has similar problems besides
 - Vice chair of Democrats abroad gave a non-answer to security questions
 - Primary vote online is public so don't have to address privacy
 - Cite use of expert vendor but no concern over track record, specifics
 - Privacy key to general election, though

Offset

Topic

21:11

- Could try public publishing of voters, votes but unconvinced this is a good idea
- Assumption is knowledge of vote could form basis of discrimination
- Citizen should feel free to vote their conscience without being penalized
- Nothing else forces someone to reveal political leanings
- Biggest limiter, yet to be addressed anywhere, is security of PC
- Easiest attack is a worm, malware, see success of Storm
- Impossible to prove after the fact that the vote is genuine
- Cost of distributing dedicate voting machines defeats the point
- No software on a general computer will ever be free of security concerns
- Life of a software engineer
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/229068544/article.pl>
 - Clearly states the problem of family, friends not understanding job
 - I had long since given up on trying to explain
 - Lays out the basics of the process well
 - In particular, when talking about requirements and design, well expresses human factors
 - Some of what he says should be considered by programmers, too
 - I have seen too much evidence of programmers ignoring customers and/or usability
 - Uses art forms as metaphors throughout
 - Also captures the fluidity of software
 - At any point, it may need to change for a variety of reasons
 - Some revision in other art forms, but there is usually a final form
 - Software changes even after this final form, patches and upgrades
 - Is an upgrade like a sequel in fiction?
 - Maybe a director's cut
 - A good balance of non-coding activities, too
 - Documenting and teaching, as well as requirements and customer wrangling
 - Not sure this accomplishes the end goal, explaining to non-coders
 - A beautiful insight into professional programming, regardless

24:48

- Study shows online gap between parents, children widening
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/229353279/article.pl>
 - The gap is between what parents thinks kids do and what they actually do online
 - Study conducted by Prof. Lemish of Tel Aviv University
 - Local study of Jewish, Arab families
 - Wonder what cultural biases, if any, are affecting results?
 - Study covers privacy, interaction with strangers, and circumventing monitors, filters

Offset

Topic

28:50

- Lemish points to poor media literacy on part of parents
- Suggests this is no different than before the internet
- Parents not necessarily aware of what goes on at clubs, school or parties
- Gives same advice as has always been helpful
- Parents should talk to their children
- Should educated, enforce the same safety rules as offline
- She thinks internet is worth the risk and parents can close the gap
- Give her credit for a constructive response, not just more chicken little reactions
- I worry a little that the potential for danger is a bit greater online
- As a parent, I suppose I can see increased risk in a number of activities
- The challenge really is the same, regardless, equip kids to keep themselves safe
- RIAA chief wants users' PC's to filter for infringement
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/231091674/20080207-riaa-boss-spyware-could-solve-the-encryption-problem.html>
 - Cary Sherman, RIAA boss, admits network filtering need not be mandated
 - Also admits it may encourage crypto arms race
 - Suggests end users should install local filters
 - Language is admittedly loaded with "could", "would"
 - Regardless, in the absence of requirement, users would not install
 - If mandating filtering is out for the ISP, why would they consider for end user?
 - Also considered installation in modem or router
 - This is no better than in the ISP's network
 - Even more ludicrous, in the P2P applications themselves
 - Filtering is solving the wrong problem
 - RIAA needs to understand why users turn to P2P and build competitive business models
 - RIAA chief was just speculating
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/231748769/20080208-riaa-president-simply-musing-about-filters-on-your-pc.html>
 - RIAA spokesperson specifically said they have no such agenda
 - Explained Sherman was just speculating
 - A few more points to consider
 - No law enforcement technique is 100% percent, why should we expect different from IP enforcement?
 - The point at which any filter scheme is effective is way beyond user inconvenience

Offset	Topic
	<ul style="list-style-type: none"> • Most telling, that this is what RIAA execs come up with when brain storming • Need to work harder to get them past control, to understand real opportunities • Labels, other players seem more receptive • Do trade organizations profit less when labels operate smoothly?
33:22	<ul style="list-style-type: none"> • <code>tail -f</code>
33:42	<ul style="list-style-type: none"> • Prentice re-introducing Canadian DMCA <ul style="list-style-type: none"> • http://feeds.feedburner.com/~r/boingboing/iBag/~3/229426563/urgent-canadians-nee.html • This law was tabled last term amidst protests • Prof. Michael Geist has the best coverage • http://www.michaelgeist.ca/ • Points out Prentice's contradictions of own party's policies • http://feeds.feedburner.com/~r/boingboing/iBag/~3/229426563/urgent-canadians-nee.html • One of the most concerning issues is lack of consultation • Citizens, researchers, consumer groups being left out in the cold • Fair dealings also under represented • Much misleading propaganda has also been published in response to protests • Geist is also doing a good job of taking that apart • Story has opportunities for action, including online groups, events and lists of MPs that constituents can and should contact
35:24	<ul style="list-style-type: none"> • EFF trying to stem tide of spurious legal wrangling by RIAA <ul style="list-style-type: none"> • http://www.eff.org/deeplinks/2008/02/arista-v-does-1-21-getting-riaa-play-rules • RIAA prosecutors asking judges to accept controversial legal theory • Not saying this theory is bad, on the face • Problem is push bypasses usual deliberation • Risk is may be distorting the law in the process • Making available argument is a telling example • Jury instruction in Thomas case, Atlantic v. Howell • EFF is filing an amicus brief in Arista v. Does 1-21 • Also looks to balance first amendment protection for anonymous speech • RIAA trying to bypass consideration of merits of case before issuing subpoena • EFF has fought for preliminary inquiry, to stall baseless suits just to unmask critics • Nice to note acknowledgement that RIAA can meet constitutional limits, that is valid • Simply trying to prevent distortion, preserve standards, limits
38:35	<ul style="list-style-type: none"> • Outro

<u>Offset</u>	<u>Topic</u>
	<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 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<ul style="list-style-type: none">• http://creativecommons.org/licenses/by-nc-sa/3.0/us/• Attribution, non-commercial, share alike