

Offset	Topic
00:17	<ul style="list-style-type: none"> • Intro <ul style="list-style-type: none"> • Out of town end of this week <ul style="list-style-type: none"> • No show 3/30 • Show as usual, 3/19
02:09	<ul style="list-style-type: none"> • Security Alerts
02:28	<ul style="list-style-type: none"> • iFrame injection attack <ul style="list-style-type: none"> • http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/253549328/20080318-ongoing-iframe-attack-proving-difficult-to-kill.html • Core attack is an injection against search engines • Adds source for a malicious iframe to cached material sent to engines • This material is served back out on same or similar keyword hits • On security researcher, Dancho Danchev, has been following closely on his blog • Attack originally used to highlight some bogus antivirus software • Also originally only targeted a couple of domains • Has moved on to other domains • Also has evolved to try to download more malware • Can be stopped at the server by simple input validation • Make sure your browser always prompts before opening files • When in doubt, refuse downloads, delete files you don't trust • Launched by a Russian commercial malware outfit, RBN • Many thought RBN had been stopped by filtering its IP addresses • Apparently subdivided and returned
04:43	<ul style="list-style-type: none"> • Evading Facebook's new privacy controls <ul style="list-style-type: none"> • http://www.cnet.com/8301-13739_1-9898098-46.html?part=rss&tag=feed&subj=SurveillanceState • Continuous with their other improvements • Superficially, a good idea • Allows user to exert more fine grained control • Can limit access to profile by types of users • Problem is other users can change their type at will • No verification of user status • So really doesn't improve privacy, any, except against naive attackers • Soghoian also warns this may encourage false sense of security • Facebook cannot really fix this problem short of vetting status • Cost to do so prohibitive for such a simple service • Also, still would not stop determined attacker

Offset	Topic
06:56	<ul style="list-style-type: none"> • News
07:10	<ul style="list-style-type: none"> • Investigation of NJ voting irregularities <ul style="list-style-type: none"> • Union County was to conduct an investigation • After errors in their presidential primary • Clerk Rajoppi asked Felten to help assess Sequoia's machine's security • Sequoia was assessed during the CA audit • It was ES&S that threatened Bowen over possible disclosure • Security researcher preemptively threatened by e-voting vendor <ul style="list-style-type: none"> • http://feeds.freedom-to-tinker.com/~r/freedom-to-tinker/~3/253302555/ • Felten published the letter he received from a VP at Sequoia • The letter was in response to NJ officials asking Felten to examine a machine • Letter is vague, but threatening • NJ county scared off audit by e-voting vendor <ul style="list-style-type: none"> • http://feeds.feedburner.com/~r/boingboing/iBag/~3/254099059/sequoia-voting-syste-1.html • http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/254928808/20080320-e-voting-blocks-e-voting-security-audit-with-legal-threat.html • Apparently send a more detailed letter to Union County clerk • Same threats as Felten's letter <ul style="list-style-type: none"> • License violation • Protection of Sequoia's IP • Threat of suit was apparently more substantial • On the advice of counsel, Rajoppi backed off • She apparently is appealing to the state's AG • Sequoia claims systems already thoroughly tested • Feels government testing less like to risk its IP • One testing lab lost its accreditation last year, however • Ars wonders why the county would acquire machines whose license doesn't allow for independent testing • More details on NJ voting irregularities <ul style="list-style-type: none"> • http://feeds.freedom-to-tinker.com/~r/freedom-to-tinker/~3/254316575/ • Felten shows direct evidence of errors • Tapes and electronic tally simply do not match • After he posted, acquire more erroneous tapes
3/20/08	<ul style="list-style-type: none"> • Sequoia's response <ul style="list-style-type: none"> • http://feeds.freedom-to-tinker.com/~r/freedom-to-tinker/~3/255064085/ • Sequoia has maintained the problem was operator error

Offset

Topic

- By their own explanation, it seems as much an engineering error
 - Seems odd that an extra button press would cause a flip to opposite ballot rather than an error or a no ballot
 - Also seems hard to credit that two views would ever be inconsistent except for an error in the code
 - No reports came in that corroborate Sequoia's explanation
 - Someone would have noticed
 - Still, seems more likely an error as an attack would have been harder to detect
 - Frustrating that vendor doesn't see its own product as flawed
 - Or even an opportunity to improve, eliminate operator confusion, error
- 12:28
- Silicon based, high temperature super conductor
 - http://www.eetimes.com/rss/showArticle.jhtml?articleID=206904213&cid=RSSfeed_eetimes_newsRSS
 - New experimental research from joint Canadian-German team
 - Using a silicon, hydrogen compound
 - Still cooled, but not super cooled
 - May lead to room temperature superconductors
 - Based on theoretical work that hydrogen will super conduct if compressed
 - Material is compressed instead of super cool
 - Broad applications, mostly where super powerful magnets are needed
 - Maybe even computing?
 - Imagine zero resistance transistors, frequency scaling no longer bounded by power or thermal concerns
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/254603363/20080319-room-temperature-superconductors-a-step-closer-with-silane.html>
 - More details
 - Compound, called silane, combusts in air
 - Pressures involved are non-trivial but lower than pure hydrogen
 - Higher temperature superconductivity occurs in critical pressure range
 - Probably not feasible for too many applications
 - Still, may point the way to future advances that would bring advantages closer
- 15:52
- CBC to experiment with DRM-free BitTorrent
 - <http://www.michaelgeist.ca/content/view/2767/125/>
 - Will be the first North American broadcaster to do so
 - A new program, Canada Next Great Prime Minister
 - Cross between reality TV, policy discussion forum
 - Will release with DRM, via BitTorrent day after broadcast

Offset

Topic

18:36

- Geist interprets this as CBC following its mandate
- To use most appropriate and efficient means to make programming available
- Makes sense for a publicly funded program
- CBC has wholly embraced podcasting
- Love Quirks and Quarks, Search Engine
- Geist also speculates choice of BitTorrent may force discussion of network neutrality
- Rogers interfering with P2P traffic may now be seen as interfering with access to information
- Seems like a good test case for P4P, if it wasn't still so early days
- Teaching a security hacking mind set
 - <http://feeds.wired.com/~r/wired/topheadlines/~3/254686862/click.phdo>
 - Explains security mindset as always consider how things fail
 - How to attack or misuse something
 - May be at odds to engineering mindset, how to make things work
 - While domain expertise, particular skills can be taught
 - Mindset itself may be innate, may present unique challenges to teaching
 - Points out a course trying to teach it
 - Student blog, posts consider security of random things
 - Thinks this can have benefit beyond IT
 - Skeptical consumers, citizens more likely to take companies, others to task
 - Anyone can encourage the mindset, just by being willing to ask the right questions
 - Goes hand in hand with his other recommendations
 - If you don't ask security questions, how can you assess the choices you are being asked to make?

20:48

- `tail -f`

21:08

- 700MHz spectrum auction conclusion, results
 - 700Mhz spectrum auction winds up
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/253895885/20080318-700mhz-spectrum-auction-wraps-up-tops-19-5-billion.html>
 - Finally tally at 19.5 billion USD
 - Bidding over the last month was slower, hit 19B in February
 - C block reserve met, activating open access conditions
 - D block reserve unmet
 - This block had emergency services infrastructure built into it
 - FCC could re-auction with different reserve, structure
 - Questions about block D of 700MHz spectrum

Offset

Topic

- <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/254381549/20080319-questions-about-block-d-linger-in-aftermath-of-auction.html>
- Promising contender, Frontline, dropped out before the start
- May have been because of conditions placed on the block
- Public Knowledge showed concerns, asked for investigation
- House Subcommittee on Telecommunications and the Internet has promised to look into it in a hearing
- Allegations of fraud around 700MHz D block
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/254877274/article.pl>
 - May be due to contractor involved in helping with the auction
 - Some allegations they spread misinformation that there would be hefty annual fee
 - D block set up as public-private partnership
 - Consulting firm representing the public half
 - Will have to wait until House hearing
- Google did not secure any of the 700MHz spectrum
 - <http://feeds.feedburner.com/~r/GooglePublicPolicyBlog/~3/255174022/end-of-fcc-700-mhz-auction.html>
 - Google congratulated the winners
 - Focused on the open access
 - May give some credence they only bid to help meet the reserve
- Verizon, AT&T win out in wireless auction
 - http://www.eetimes.com/rss/showArticle.jhtml?articleID=206905006&cid=RSSfeed_eetimes_newsRSS
 - Both will use the new spectrum to supplement existing offerings
 - No new nationwide, wireless broadband
 - Some smaller players also secured licenses
 - Martin things competition was preserved
 - I rather doubt it
 - Verizon does seem to be committed to open access, though
 - Exact conditions of device certification still unclear
 - Between two of them, accounted for 16B of the bids

27:06

• **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

Offset**Topic**

- 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