

Offset	Topic
00:17	<ul style="list-style-type: none"> ● Intro
	<ul style="list-style-type: none"> ● USACM meeting <ul style="list-style-type: none"> ● A wide variety of issues ● Filters, an extension of DRM argumnet ● Privacy, security and surveillance ● Quite a bit of time on e-voting ● Considering more than just the security ● Open government, transparency
04:54	<ul style="list-style-type: none"> ● Listener Feedback
	<ul style="list-style-type: none"> ● Jon I. <ul style="list-style-type: none"> ● Facebook message ● DTrace was developed by Sun ● For Solaris ● Not for linux by open source hackers ● Site comment on using Vorbis to avoid patents
08:47	<ul style="list-style-type: none"> ● Security Alerts
09:07	<ul style="list-style-type: none"> ● New web security scanner from cDc <ul style="list-style-type: none"> ● http://feeds.feedburner.com/~r/boingboing/iBag/~3/238000039/goolagorg.html ● A standalone windows gui ● Uses Google with "dorks" ● Canned search patterns that may reveal security problems ● Is really similar to other scanners, like nessus ● Dorks are like plugin but simpler ● Expressed in simple XML file ● Google hacking is not new ● Haven't seen as much about hardening against hacks ● Maybe the presence of an automated tool will pressure providers
11:26	<ul style="list-style-type: none"> ● Troubling paper on security issues with wireless implementations <ul style="list-style-type: none"> ● http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/237129580/20080218-report-implementation-flaws-hound-wireless-security.html ● That WiFi implementation have flaws is not news ● Popularity of WiFi makes this concerning ● Perception that just enabling WPA grants security is also problematic ● Also a concern for emerging standards, like WiMax ● Codenomicon work uses its own tool ● Fuzzes several technologies to try to uncover implementation flaws

Offset

Topic

- Attacks on implementations more common, effective than on design, protocol
- Highlights additional risks of wireless
 - Always on
 - Open physical access
 - Anonymity
 - Some of these are true of TCP/IP in general
 - Speaks more to these aspects in physical space
 - Also opens direct attacks, outside of the network itself, difficult to detect, identify and foil
- Even taking with a grain of salt, results are concerning
- Would like to see third party verification, many hackers accomplished at fuzzing
- Would Codenomicon share details, perhaps under NDA, for purposes of verification?
- Are wireless implementers skipping security assessments as part of QA?
- Protocol based products in particular need wider, more comprehensive testing
- Not just robustness of protocol to noise, normal but also fuzzing, other attacks
- Would have been nice to see some recommendations on vendors, products that do well

15:26

• News

15:40

- Quantum computers may not be as powerful as expected
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/237499936/article.pl>
 - Takes exception with simplistic claims
 - Identifies several areas that would be adversely affected if true
 - Mathematics, could brute force searches
 - AI, could brute force parameters for neural nets
 - Many credible sources are skeptical
 - Nobel laureate Robert B. Laughlin
 - Computer scientist Leonid M. Levin
 - Even while attempts to build have been limited
 - Theoretical research has tried to identify at what a quantum computer would excel
 - Some criticisms, like error correction, have been met
 - If others prove it impossible, may be more telling for correctness of quantum mechanics
 - Identifies computation complexity as the key challenge
 - Applies to both types of computing
 - One of the hypothesis of quantum computing is it will classes of complex problems more efficiently than classical counterparts
 - Gives a good, approachable treatment of complexity

Offset

Topic

- Challenges apply to any non-classical computer, say a super string or relativity computer
- Question really us how efficiently can the universe itself compute
- Current research seems to indicate that NP-complete problems can be solved in polynomial time
 - Polynomial just means raised to a discrete exponent
 - NP just means a solution can be recognized in polynomial time
 - Solution time may be infeasibly large, unknown
- Also gives a good primer on quantum mechanics
- Covers the math in an accessible way
- Deconstructs Shor's algorithm for factoring large integers
- Turns out it relies on unique aspects of that problem
- Is not NP-complete, so doesn't say anything about general power of quantum computing to arbitrarily complex tasks
- There is some research that proves QCs may be generally a bit faster
- But not the giant leaps often claimed by proponents
- Does a fair job of outlining what may be the physical limits of computing
 - Smallest unit of time seems to be the Planck time
 - Clock ticking out that unit would need so much energy it would collapse into a black hole
- Even entertains some science fictional extrapolations
- Adobe pushing DRM for Flash
 - <http://www.eff.org/deeplinks/2008/02/adobe-pushes-drm-flash>
 - Flash video, FLV, has cracked the nut of streaming
 - No plugins, no special software
 - Many sites use it, most don't bother to protect it
 - Many extract the video and re-mix
 - In Flash 9 and the 3rd version of the server software, Adobe will add DRM
 - No one expects it to be unbreakable
 - Will trigger DMCA complaints
 - Clauses against tools for circumvention may chill legit 3rd part tools
 - Seth Schoen suggest this may also stall media literacy efforts
 - Argues that unencumbered web hosted video is pick up slack where other sources are failing
 - Similar to Lessig's thoughts in Free Culture, remix to learn language to understand what you are seeing, consuming
 - As with DRM elsewhere, forestalls any attempt of a fair use defense
 - Same anti-DRM arguments apply
 - Arguably, fluidity, low friction of FLV has enhanced its success
 - Interfering with how easily it spreads could stall its own popularity

23:15

Offset

Topic

26:48

- Biggest obstacle to it killing itself is how much content may be locked up already
- If DRM can be applied after the fact, trouble; not sure that's how it will work
- Antithetical to Adobe opening up some of its other web focused code
- This will serve the few, the consolidated media interests, at the expense of the many
- The socio-economics of Lego bricks in the classroom
 - <http://blog.wired.com/geekdad/2008/02/lego-building-a.html>
 - Clearly a microcosm of real society
 - Fascinating to see a beloved childhood toy in this way
 - Utility still matters as the group expression is building
 - Potential of certain pieces, "cool" ones, drives exchange rate
 - Authors reveal their bias
 - Statement about a capitalist market driven society being unfair
 - In their decision to remove Legos, seem honest about those biases
 - Also intriguing to see kids thinking politically
 - Often think of politics as something informed from the outside
 - When resources are scarce, economics and politics emerge from simple interactions
 - Children were unconsciously influenced by the world around them, though
 - Teachers were bold to realize the opportunity to introduce other ideas
 - Social justice, collective good
 - Did a good job, I think, in deconstructing the issues at play
 - Re-introduced the legos after exploring structures of power, ownership independently
 - Also raised consciousness of choices of politics, economics
 - One very compelling point they tried to teach about unfair systems and change
 - Systems are created by people
 - They can be challenged and reformulated
 - Seems this might have some similarity to creating free, open licenses
 - No one knows ahead of time what will work
 - Some experimentation, trying to create fair, equal opportunities
 - This is all at an after school program
 - I think this would be worthwhile in regular curriculum
 - Would teach history, politics, economics in a more direct way
- Cold reboot attack on disk encryption
 - <http://feeds.freedom-to-tinker.com/~r/freedom-to-tinker/~3/238846476/>
 - Drive encryption is recommended for several reasons

30:59

Offset

Topic

- For portables, to protect data in case of loss
- With some over-reaching searches, also to protect data
- Received wisdom is it is harder to circumvent
 - Master keys only stored in volatile memory
 - Protected by operating system
 - Cut power to remove operating system deletes keys
- Felten, Halderman, Schoen, Heninger, Clarkson, Paul, Calandrino, Feldman, Applebaum
- Demonstrated an effective attack on most popular drive encryption schemes
- Info in DRAM fades gradually, not instantly
- Cooling can extend fade period, preserve info
- Using liquid nitrogen, can preserve for hours
- Even compressed air sprays can preserve long enough, minutes, to exploit
- No safe place to store master keys
- No easy way to address
- Even trusted computing doesn't help
- Video at paper site describes the research pretty well, accessibly
- I wonder if this has broader applications?
- What else could be stolen from fading DRAM?
- Would this be effective for espionage?
- Fix will require change by vendors
- May involve password protecting keys but that may not always be practical
- Would require use prompt before reading disk, may not always be possible

34:57

- **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