

Offset	Topic
00:17	<ul style="list-style-type: none"> • Intro
	<ul style="list-style-type: none"> • CBC Radio One drops Search Engine
02:22	<ul style="list-style-type: none"> • Security Alerts
02:41	<ul style="list-style-type: none"> • A couple of Firefox 3 bugs already <ul style="list-style-type: none"> • http://go.theregister.com/feed/www.theregister.co.uk/2008/06/19/firefox3_bugs/ • This is an unspecified flaw, reported by vendor TippingPoint • Apparently received through their zero-day bounty program • No further substantiation of the bug • Flaw apparently allows hostile code injection, so pretty severe • Affects Firefox 2 as well, not just the new 3 • TippingPoint withholding details until Firefox developers issue a patch • Also this week, a posting on a security list of a buffer overflow • Unclear if this is the same bug • Posting only mentions Firefox 3, not enough to rule out it also affects 2 • High risk vulnerability in Firefox 3 already <ul style="list-style-type: none"> • http://feeds.downloadsquad.com/~r/weblogsinc/downloadsquad/~3/316338151/ • More details on bug from TippingPoint • To be at risk, need to visit a malicious site and click an infected link • Mozilla already planning to include a fix in 3.0.1 update
05:17	<ul style="list-style-type: none"> • Listening to encrypted VoIP without decrypting it <ul style="list-style-type: none"> • http://technology.newscientist.com/channel/tech/dn14124-compressed-web-phone-calls-are-easy-to-bug.html • New Scientist article • Encryption in VoIP has been touted as a means to protect against illegal wire tapping • Many services use or plan to use compression • Help offset bandwidth consumption • According to research at John Hopkins VBR compression is a problem • Detectable patterns survive encryption • The variation in bits used for spoken words is regular and predictable • Research isn't up to recovering conversations • Can detect phrases, though, by building a comparison phrase, compressing and encrypting

Offset

Topic

- Average detection rate is only about 50%, jumps to 90% with longer keywords, like jargon
- Says to me that there may be significant challenges to full recognition or arbitrary filtering
- Still, this is similar to frequency analysis for simple text ciphers
- Makes you wonder that it hadn't been identified sooner
- Still, a risk worth being aware of
- Using constant rate compression would eliminate the possibility
- Would be good to see VoIP vendors include that in security considerations

09:27

• News

09:41

- Top woman coder explains gender inspired differences in code
 - <http://blogs.wsj.com/biztech/2008/06/06/men-write-code-from-mars-women-write-more-helpful-code-from-venus/>
 - Emma Grattan, VP of Engineering at Ingres
 - Ingres is venerable database started at Berkeley
 - Now a commercially supported open source database
 - Spawned many other databases, included SQL Server and PostgreSQL
 - Believes men and women write code differently
 - Women are more considerate of others who will read, follow
 - Leave directions, explanations; better capture intent
 - Thinks men want to show how clever they are
 - Write more cryptic code
 - Says she can see the difference and accurately guess gender 70%-80% of the time
 - Institute standards to run out gender differences
 - Include file or type level comment
 - Also detailed history
 - Isn't that what revision management software is for?
 - I am unconvinced this is entirely a gender issue
 - I think less seasoned developers fixate on cleverness, ignore good comments
 - More experienced start to appreciate that roadmap affect
 - If women are more open to the latter style of development, then the industry should preferentially hire
 - Coding standards are only a partial answer
 - Need to mentor developers to appreciate enlightened self interest
 - You will need to maintain your own code
 - After several months away, you will appreciate better guidance, explanation of intent
- UCITA sneaking back inside anti-spyware bill
 - <http://www.gripe2ed.com/scoop/story/2008/6/16/1219/71034>

13:53

- UCITA was a federal bill considered in the late 90s
- <http://en.wikipedia.org/wiki/UCITA>
- On the surface, seems like an acceptable idea
- Would introduce standards around software licenses, sales and other commercial practices
- Problem is that the bill, as proposed, allowed vendors to remotely disable their software
- Justification was self-help when piracy was suspected
- Bill was ultimately defeated but passed in two states, MD and VA
- This "self-help" appears to be sneaking back in inside an anti-spyware bill
- Counter Spy Act, introduced by Senator Mark Pryor, D-AZ
- US Senate Committee for Commerce and Transportation held a hearing on the 11th to discuss issues, hear testimony about bill
- Very similar to poor Can-Spam act, article itemizes problems
 - Basically, consumer isn't given any additional tools
 - Doesn't really change what is and is not illegal
- Troubling part is section 6a
- Grants exemptions to vendors when using remote monitoring for several purposes
- Includes network security, troubleshooting but also explicitly states for addressing issues of unauthorized use
- Representatives of BSA are lauding this section, in particular
- Raises the question of the real goal of the bill; anti-piracy or pro-privacy?
- Americans for Fair Electronic Commerce Transactions, AFFECT
 - Organization that helped defeat UCITA
 - Speaking out on section 6a, too
 - Points of ambiguities of authorized use, that this is more suitable for judicial review
- Article also points out that spyware authors often try to claim legitimacy
- Further muddies the waters as they may claim what they are doing is legal
- AP to discuss guidelines, compromise with bloggers
 - http://feeds.wired.com/~r/wired/topheadlines/~3/313791659/AP_BLOGGERS
 - Story started with AP claiming copyright infringement over a blogger quoting their stories
 - Specifically sent a legal notice to Rogers Cadenhead, the author of The Drudge Retort
 - Cadenhead complied with notice, citing hassles for a small player to deal with a potential court case
 - My impression is AP wants to exclude bloggers unilaterally, or at least control who can use what

- Sounds like a fair use case to me, at best AP would need to file specific complaints
- Would be up to a judge to decide infringement vs. fair use
- Another case of a business feeling threatened, wanting the law to protect them from change, in this case bloggers as distributors of news
- Now trying to craft guidelines for use
- Problem is, such guidelines still should and cannot trump fair use
- Idea is not entirely novel, Creative Commons is a general license, conditions for use without explicit consent
- CC doesn't go against copyright, however, actually relies on it
- AP claims concern over both dilution of business and journalistic integrity, i.e. risk of material quoted out of context
- This is not novel, should be legal, other recourse
- Cadenhead and representative from bloggers group were positive about guidelines from AP
- More details on bloggers association
 - <http://feeds.feedburner.com/~r/boingboing/iBag/~3/315315588/who-are-the-media-bl.html>
 - Some question of just how much the Media Bloggers Association represents general interests
 - Teresa Nielsen Hayden did some research, seems to indicate the group is one blogger
 - Right wing attack blogger
 - However, commenter claims other key bloggers have been involved with MBA
 - Says the associations involvement in past instances has been helpful
 - Her post also clarifies that Cadenhead requested MBA's involvement
 - And that news stories are misrepresenting participation of MBA
- House passes telecom immunity bill
 - <http://www.eff.org/press/archives/2008/06/20>
 - Bill positioned as a much needed update to FISA procedures
 - Rushed to a vote after introduction
 - Never a good sign
 - Passed by over a two-thirds majority
 - Requires dismissal of existing suits against telcos
 - Allows telcos to be given immunity with a simple memo from the executive
 - Unclear if this would only apply to existing activities or apply in the future
 - EFF correctly identifies certain risk
 - Will lose ability to discover full scope of domestic wire taps
 - Goes to vote in the Senate next week

Offset	Topic
26:56	<ul style="list-style-type: none"> • Use EFF action center to ask your senators to vote no • Requires a call, so act promptly • I intend to call tomorrow morning • Read elsewhere that Obama supports the bill though he opposes the immunity provision • Says he will fight to remove the provision • Will vote yes even if he cannot get the provision removed, though • Why are otherwise sane Congress critters so willing to give up?
27:16	<ul style="list-style-type: none"> • tail -f • Dodgy interview with Prentice on C-61 <ul style="list-style-type: none"> • http://www.cbc.ca/searchengine/blog/2008/06/jim_prentice_unlocked_the_sear.html#more • The impression I get is that Prentice doesn't fully understand the bill • Made his question to Jesse about him reading it a bit hypocritical • Legal scholars, like Geist, are still reading it • Was genuinely evasive on issues of DRM trumping user rights • A bit naive about market sorting things out • Suggested at one point that music industry is abandoning DRM • Then why legislate anti-circumvention measures? • Was a bit rude, but did say he only had ten minutes • Warned repeatedly he had to go before he did hang up • The fact that he could not articulate a simple set of goals, principles suggest to me he just adopted what industry asked • Kept saying it was complicated, didn't even re-iterate the simple view expressed in the backgrounder
29:37	<ul style="list-style-type: none"> • Professors back Thomas on flawed jury instruction <ul style="list-style-type: none"> • http://feeds.wired.com/~r/wired/topheadlines/~3/315047726/professors-sidi.html • When Judge Davis said he erred on the jury instruction about making available, invited comment • Will hold a hearing in August • So far, first and only responders are a group of ten copyright scholars • Not any I recognize, either, so its not just the usual suspects • Strongly state proof of transfer is required • Based on review of the statute • One of the scholars even stepped forward on the issue of RIAA downloads as proof • Said verdict could stand on 24 downloads • Rejects that these count as they are authorized by industry • Article admits that proving a genuine, 3rd party transfer is technologically infeasible • How does that square with unquestionable rights against real piracy, then?

Offset**Topic**

- The constructive answer is it is moot
- Industry needs to spend those resources competing with P2P, not stifling it

33:20**• 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