

Offset	Topic
00:17	<ul style="list-style-type: none"> • Intro <ul style="list-style-type: none"> • iPod Touch <ul style="list-style-type: none"> • First got to play with one a few months back • Immediately so the potential for a nice net appliance • The 32GB has enough space for my library • Already using it instead of my laptop for trivial things • Checking twitter, occasionally looking things up • At Balticon was able to use it to stay connected everywhere • I have a crappy cell phone • I hate cell phones, this is the most I will buy • As a consequence, doesn't work a lot of places • I like how the touch complements SMS where there is WiFi • The music interface is just different enough it is taking some getting used to • Not all information is available, lost release date, show notes from podcasts • Using touch interface without looking is almost impossible
05:38	<ul style="list-style-type: none"> • Security Alerts
05:57	<ul style="list-style-type: none"> • Vulnerability in popular cell phone <ul style="list-style-type: none"> • http://go.theregister.com/feed/www.theregister.co.uk/2008/05/28/razr_security_jpg/ • Problem is in the EXIF parser used in supporting JPG • EXIF is embedded metadata in image • An malformed file can be sent to a Motorola RAZR via MMS • Could cause overflow, arbitrary code execution • Problem was originally reported late last year • Motorola just now has issued a new firmware version to address • May be complex to exploit but only requires one person to write automated attack • Not entirely sure of value in attack • Personal data for sure • Could an attack coopt a phone for other use like SMS spam? • Mobile botnet? • Article doesn't entertain speculation • Mobile devices increasingly more attractive with rise in popularity • Not necessarily harder to secure but appearance of being more closed • Phones provide more and more general facilities, though, like email, web browser • Equally capable for attackers to exploit

Offset

08:27

Topic

- SSL black list extensions for Firefox detects bum Debian certificates
 - <http://feeds.downloadsquad.com/~r/weblogsinc/downloadsquad/~3/300653302/>
 - Comment on the web site gives more details
 - http://thecommandline.net/2008/05/18/news_141/#comment-13563
 - As a system administrator solution is to update, regenerate keys
 - As a user, what can you do?
 - Firefox extension helps users identify potentially bad keys
 - <https://bad.codefromthe70s.org/>
 - URL with know bad key for an example
 - <http://codefromthe70s.org/sslblacklist.asp>
 - More details at developers site
 - Collecting a database of know bad certs
 - Can report sites through the extension itself when it identifies a bad cert
 - Based on database released by Ubuntu folks of finger prints of bad keys

11:26

• News

11:40

- Formal practice exercises for coding
 - http://www.hackszine.com/blog/archive/2008/05/code_kata_exercise_for_the_sof.html?CMP=OTC-7G2N43923558
 - Idea borrowed from martial arts
 - Preset forms of practice to help improve skill
 - Site explains also that many programmers have only theoretical knowledge
 - Learning on the job means making mistakes in production code
 - Separating practice out allows for improvement not at the expense of live code
 - Code exercises that are 30 to 60 minutes long
 - Some are programming, others are open ended thought exercises
 - There is also benefit in practice without pressure, deadlines
 - Implication is that trying to learn under pressure is not ideal
 - I'd have to agree, may not appreciate full nuance when just trying reach a goal quickly
 - Also emphasizes feedback, focus is on correcting, improving
 - Incidental learning, too, not just arriving at correct answer
 - First 21 katas are a good mix of the practical and conceptual
 - Reviewed a few, these are close to problems I've had to solve
 - Strongly recommend not only giving these a try but using them to recognize opportunities for learning in your regular work

14:50

- TJX fires employee for discussing lax security
 - http://www.theregister.co.uk/2008/05/23/tjx_fires_whistleblower/

Offset

Topic

19:30

- From the article, it sounds like this employee tried to work within the system
- Problems appear to go back well before the data theft
- Very little positive response from the company
- A brief period of stronger passwords following a known breach
- Some question his actions
- Were they the best way to bring attention to the issue?
- Others consider him a whistle blower
- Given the non-responsiveness of the company, I tend to agree with the latter
- Benson, employee, highlights it is not just the company's assets at risk
- Employee and customer data also at risk
- Arguably the data breach shows this is the bigger risk
- What else could Benson do given the lack of action?
- Meshes with the question of how to make companies behave more responsibly with consumer data
- Consumers not in a position to know security details
- If employees are but can be so easily dismissed, how do we expect things to improve?
- TJX had an opportunity to turn this into positive PR
- Instead, they just received another black eye
- Neuros brings VideoLAN into device market
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/300128483/article.pl>
 - Will involve maintainers from the VLC project itself
 - Part of Neuros' efforts around an open hardware platform developing in partnership with TI
 - VideoLAN will pretty much form the heart of the box
 - Provides encoding, transcoding and playback
 - Has a well established plugin design for new codecs
 - From the article, seems to take good advantage of Linux and the hardware
 - All porting efforts will be shared back into the VLC project
 - Neuros is making very good on its promises to popularize open source in this space
 - VLC is a quiet but strong player
 - Personally, I have found very little content with which it could not deal
 - Should by now use it first, but always end up using as a more capable fall back
 - Curious to see if anyone else makes use of this ARM port
 - In particular, the port would be a free way to bring Ogg support to new devices

Offset	Topic
25:46	<ul style="list-style-type: none"> • Really want to see if the forthcoming box can deal with digital content • The existing Neuros offering is limited to analog capture, RCA or S-video connection • Will certainly do well with downloaded content of all varieties • MediaDefender attacks legitimate IPTV player, Rev3 <ul style="list-style-type: none"> • http://revision3.com/blog/2008/05/29/inside-the-attack-that-crippled-revision3 • Rev3 uses BitTorrent to legitimately distribute its video content • Experienced an outage over the Memorial day weekend • Good explanation of a syn flood attack • Rev3 performed its own investigation to uncover DDoS • Identified Media Defender who had worked for several labels and both MPAA and RIAA in the past • Not to be confused with Media Sentry, which is an investigator • Media Defender pollutes, attacks P2P networks • Was subject of much press, ridicule in wake of an email leak earlier in the year • Execs admitted to attacking trackers over past months • Apparently using a back door in the tracker • Claim flood was initiated by Rev3 corrective action • Doesn't claim a specific attack or any responsibility • Unclear why they were injecting their own torrents except to cause Rev3 problems • Maybe because they automatically identified the server as an open, public tracker • Media Defender claims they will check with operators in the future • Attack took out all of Rev3, not just their tracker • Despite Rev3 CEO's unwillingness to speculate, does think what Media Defender does is wrong, penalizes anyone using protocol regardless of actual use • http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/300911949/20080529-revision3-ceo-blackout-caused-by-mediadefender-attack.html • More explanation of what Media Defender does more generally • More details on Media Defender getting caught doing suspicious things
30:26	<ul style="list-style-type: none"> • <code>tail -f</code>
30:45	<ul style="list-style-type: none"> • NBC, MS claim to have gotten to source of broadcast flag snafu <ul style="list-style-type: none"> • http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/300662814/20080529-concerns-linger-in-wake-of-nbcwindows-mce-recording-snafu.html • NBC still claiming this is an accident • Microsoft has yet to explain why they are obeying the flags • Was apparently a flag for analog, not digital content

Offset

Topic

- Flag in question has three settings, copy never, once or freely
- Inadvertently set to copy never
- Claim since this is an analog only flag, will never happen after the digital cutover
- Microsoft also making noises about preventing error
- How about patching the software to eliminate the possibility?
- Both are concentrating on procedural or administrative fixes

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