

Offset	Topic
00:17	<ul style="list-style-type: none"> • Intro
05:20	<ul style="list-style-type: none"> • Security Alerts
05:39	<ul style="list-style-type: none"> • Security suite running on an OpenMoko phone <ul style="list-style-type: none"> • http://rss.slashdot.org/~r/slashdot/eqWf/~3/MNBvFgC-9lg/article.pl • Similar to BackTrack Linux, Live CD distro built with security testing in mind • http://en.wikipedia.org/wiki/BackTrack • Existing security software customized to take advantage of Neo's hardware • neopwn sells OpenMoko phone's pre-installed • Also sells software bundle • Looking to build a wiki, a support community • Also added automation to make running tests easier • To help overcome limitations of touchscreen keyboard • Project also offers a netbook loaded with similar tools • Clearly hiding the phone makes attackers less conspicuous • Like software tools, should encourage organizations to take security very seriously • For professionals, lowers cost, complexity
08:15	<ul style="list-style-type: none"> • New browser exploit, "clickjacking" <ul style="list-style-type: none"> • http://blogs.zdnet.com/security/?p=1972 • Affects all major browsers, latest versions • Was going to be presented about recently but canceled at behest of vendors • Researchers, Robert Hansen and Jeremiah Grossman, have released some info, anyway • Has nothing to do with JavaScript • An attacker can pretty much take over what links your browser clicks • Some vendor patches are starting to come in, issue is deep, though • You have to click for the attacker to redirect, though • Flash and JavaScript make it easier • Sounds like a flaw in DHTML, maybe event bubbling in the DOM? • Researchers say turning off all plugins, scripts is only protection • Author of NoScript, Giorgio Maone, offered some good news • http://blogs.zdnet.com/security/?p=1973 • Default NoScript config will foil most attacks • Check PluginsIForbid iFrames for complete protection • Cause of clickjacking remains unknown

Offset

Topic

- <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/94ahC-pl7ME/20080926-new-clickjacking-affects-all-browsers-cause-remains-unknown.html>
- Researchers pulled own talk after learning Adobe product may be affected
- Trying to be responsible in disclosure
- Only pure text browsers, like lynx, unaffected as they have no click events
- Attack is not new, apparently, but risk is not being fully appreciated
- Lack of details leads author to speculate exploits in the wild may be thin
- Zero Day does cite some proof of concept code, though
- At least Adobe is aware of it and working of fix
- Hopefully browser developers are as well

11:58

• News

12:13

- German developer strips privacy concerns from Chrome to produce Iron
 - <http://feeds.downloadsquad.com/~r/weblogsinc/downloadsquad/~3/401972241/>
 - Even though Google removed copyright license from EULA
 - Still likely to be collecting some anonymous statistics
 - In particular for location bar auto complete
 - German government issued a warning against Chrome for privacy concerns
 - SRWare, a German developer, modified Chromium
 - Stripped out identifying information
 - Disabled info being sent to Google, even crash reports
 - Took out Google updater
 - Otherwise seems to work just fine
 - Clearly an advantage of open source of Chromium
 - Chrome is not unique with these concerns, though
 - I am unaware of an altered build of Firefox for this reason
 - There are extensions to accomplish those, though
 - Stealther, for one, also 3.1 will come with a private mode
 - I think the pressure for Google, others to collect data is only going to grow
 - Some sort of compromise is going to be necessary
 - Especially with the collector now subsidizing a browser
 - The key question is how do users audit that collectors are being honest
 - Thankfully, there is a motivated hacker community that can and will do so
 - Tech press also likely to shed light on results, good or bad
- Muxtape may be another pirate's dilemma

16:20

- <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/NjjQu1an6XA/20080923-muxtape-may-be-dead-but-it-lives-on-through-its-children.html>
- Muxtape started by hosting playlists
- The idea was like exchanging mix tapes back when cassettes were really only writable audio media
- Got shut down by RIAA when started hosting actual audio files
- Has inspired imitators looking to fill the need, avoid the trap
- MixTube uses YouTube infrastructure
- Pushes logistics, legal worries onto YouTube
- Favtape hosts playlists, imports from last.fm, Pandora
- Uses seeqpod to find tracks all over the public internet
- seeqpod also in trouble with labels
- Favtape, seeqpod try to evade issues by claiming to be just search engines
- Like PirateBay, do not host anything, just help users find it elsewhere
- Labels think returning infringing material as majority of results is comparable to directly hosting
- Songza mixes both approaches, serving from YouTube
- Finds songs elsewhere when YouTube doesn't have track
- Pays to collecting societies, unlike MixTube, FavTape
- Hard to see any of these as replacements for downloads
- Are all streaming, cannot take music with you
- Like Pandora, serving a need the industry is under serving
- The quick appearance of clones reinforces the point
- Similar to Napster and its work-a-likes
- Labels could control their own online destiny
- If any of them offered similar capabilities out of their massive catalogs
- Could drive download sales
- Open source life streaming
 - http://www.hackszine.com/blog/archive/2008/09/sweetcron_open_source_lifestre.html?CMP=OTC-7G2N43923558
 - Life streaming has emerged as a way to consolidate social network services
 - Provides a single place for people to read all your updates
 - Some also provide an additional conversation channel
 - In my experience, some people like, some hate
 - Enough prefer it that many have popped up
 - Sweetcron is the first open source one
 - Can self host, own your own your own lifestream data
 - You have to self host, at the moment
 - If it is well received, providers may start to offer, like WordPress

Offset

Topic

25:54

- You can also modify appearance, function to suit
- Part of what I dislike about FriendFeed is the network on top of lifestream
- See way to much cross chatter
- In my view, doesn't make it easy enough to ignore Foaf data
- Sweetcron seems to eschew network, is more like a single author blog
- With separate RSS feeds for each friend, would seem easier to manage
- Licensed under GPL v3, but not Affero GPL
- Regardless, could enable new uses closed lifestream apps do not
- Should make it easier to adopt new sources to pull in
- Has a plugin architecture, as well as supporting explicit themes
- With slow adoption of OpenSocial, data portability, this seems like a good workaround
- Let users self host, make installation, customization simple enough for folks used to hacking on WordPress or MT
- Adobe's reasoning for keeping Flash closed
 - http://go.theregister.com/feed/www.theregister.co.uk/2008/09/26/adobe_google_mozilla_tensions/
 - Flash is ubiquitous, whether you like it or not
 - Google seems to like it but isn't backing it, outside of YouTube
 - Their open web advocate, Dion Almaer, cites the closed source of the player
 - Adobe's response has been that the tools, Flex, are now open
 - The file format, SWF, is also open
 - Says it is unlikely the player will be opened
 - Adobe's McAllister cites proprietary codecs as one reason
 - Adobe licenses them then gives them away
 - They don't think this would work with an open source player
 - McAllister also points out there is an open, transparent community around Flash
 - Everything but the source, basically
 - McAllister thinks Java's decision, success had more to do with a slowing market
 - Implication is Flash is anything but slowing
 - Sun did show that codec licenses could be cleared or re-written
 - Linux kernel has straddled proprietary device drivers
 - Not ideal, but another model that could be explored for codecs
 - Cites others taking advantage of open source, to Adobe's detriment
 - Using a share-alike license could ensure Adobe benefits as much as anyone from work of others
 - Seems like Adobe's problematic efforts could have done with a better license choice

Offset

Topic

- The case in point is TraceMonkey, which is surprising
- Still sounds like this is a specific negotiation, license failure than a general flaw of open source
- Mozilla also sees the collaboration differently, that they are contributing back
- Final reason is fragmentation, compares it to state of browsers
- That one may be the most fair as the sole benefit of closed source is Flash is the same everywhere
- With competitive offerings like SilverLight and JavaFX, though, some fragmentation is being attempted
- If Adobe maintains the gold standard, there may be little reason for this to change
- With Microsoft's reluctance around open source, unlikely they'd try to build their own Flash just for MSIE
- If end users had to install Flash in MSIE, though, it would seriously erode the appeal
- Could work with WHATWG to get Adobe ideas, technology adopted as part of HTML 5
- Would only work if they were willing to open the relevant parts of Flash
- Canvas tag and SVG have been trying to provide an open replacement to Flash for a while
- Could cooperate with that rather than compete

32:03

- `tail -f`

32:22

- DoJ enforcement dropped from IP Enforcement bill
 - <http://www.eff.org/deeplinks/2008/09/doj-agrees-ip-enforcement-bill-bad-idea>
 - DoJ sent a letter echoing concerns of EFF, other groups
 - Despite fast tracking of bill, civil enforcement provisions have been dropped
 - Bill has been unanimously passed by the Senate in this form
 - More on IP bill passing Senate
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/YQec21fjHic/20080926-ip-bill-passes-senate-no-civil-enforcement-power-for-doj.html>
 - Creation of copyright czar within the White House remains
 - Oddly enough, White House objects to this
 - House version of the bill passed in May
 - With latest changes, the two bills largely match
 - Much remains else remains, especially increase in penalties
 - House will have to pass the new Senate language, not much resistance is expected

33:55

- Senate updates rules on members use of internet services

Offset

Topic

- <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/uuQg6yPh7aE/20080925-senate-boldly-advances-to-2005-with-updated-web-linking-rules.html>
- Only amends policy to allow linking
- Not as comprehensive as what Culbertson called for
- No authorization of third party services
- Unclear how this will work with embedding such as YouTube
- Former ban was largely ignored, anyway
- If the changes still don't track use, well, may still be ignored
- Understand concerns about commercial, political influence
- Government should look into open source solutions
- laconica.gov.us and sweetcron.gov.us
- Would provide channels without influence
- Government, congress critters would own data

36:28

• **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