

| Offset | Topic   |
|--------|---|
| 00:17  | <ul style="list-style-type: none"> <li>• <b>Intro</b> <ul style="list-style-type: none"> <li>• Correction on pronunciation of Levy's name</li> <li>• Help with my next promo</li> <li>• Submit application or recommend contributors for OMR</li> </ul> </li> </ul>   |
| 03:13  | <ul style="list-style-type: none"> <li>• <b>Security Alerts</b></li> </ul>  |
| 03:32  | <ul style="list-style-type: none"> <li>• Demo of direct, remote attack against Intel chips <ul style="list-style-type: none"> <li>• <a href="http://rss.slashdot.org/~r/slashdot/eqWf/~3/335409428/article.pl">http://rss.slashdot.org/~r/slashdot/eqWf/~3/335409428/article.pl</a></li> <li>• Researcher Kris Kaspersky to demonstrate attack</li> <li>• At Hack in the Box in October</li> <li>• Based on flaw in Intel chips, exploitable with JavaScript or plain TCP/IP packets</li> <li>• Article is a bit confused, mentions JavaScript, then Java</li> <li>• Simply is a demonstration of how to use known errata about chips</li> <li>• Can cause both crashes as well as arbitrary code execution</li> <li>• Since these are flaws in the chip, bypass OS security</li> <li>• Some can even be used to subvert OS security</li> <li>• Researcher is apparently critical of industries handling of errata</li> <li>• Implication is they should be more proactive to use BIOS workarounds</li> <li>• Many do not</li> <li>• Very much reminds me of panel with Vinge</li> <li>• Unintentional breaks but in critical class for computing infrastructure</li> <li>• May seem obscure, but only takes one to write attack</li> <li>• Author doesn't need to deploy, others can use existing code, can even be deployed in self replicating code, worm</li> <li>• Can't exactly upgrade a processor for security fixes</li> <li>• If vendors pay attention to errata, may be able to upgrade BIOS as effective fix</li> <li>• Otherwise, based defense is like any, be careful what you trust, use a router/firewall to foil remote packet attacks</li> </ul> </li> </ul> |
| 06:49  | <ul style="list-style-type: none"> <li>• Fall of CAPTCHAs <ul style="list-style-type: none"> <li>• <a href="http://rss.slashdot.org/~r/slashdot/eqWf/~3/336442258/article.pl">http://rss.slashdot.org/~r/slashdot/eqWf/~3/336442258/article.pl</a></li> <li>• Quicky history, developed in 2000 by CMU researchers</li> <li>• Distorted strings of characters, supposedly only decipherable by humans</li> <li>• Quickly and widely adopted</li> <li>• This year, though, the most high profile captchas have failed</li> <li>• Yahoo mail, Gmail, Hotmail</li> <li>• Attacks have been automated so any spammer or attacker can benefit</li> </ul> </li> </ul>   |

## Offset

## Topic

- Many different options, actually, from free to commercial
- Targets are too attractive, article highlights examples
- In the case of Gmail, not just a trusted email
- Clever attackers also using other Google offerings, like Docs to deliver malware
- Even newer approach, creation of quick web sites, like Google Sites, etc.
- Conclusion is captchas are a dead solution
- Implication is focus on them has stalled progress
- Thinks concept may be valid but clearly needs to be fresh research
- Is an arms race, is always going to be a need for next thing

10:41

### • News

10:55

- Blizzard wins motion against Glider developer
  - <http://virtuallyblind.com/2008/07/14/blizzard-wins-sj-mdy/>
  - MDY created software called glider
  - Essentially a bot to drive WoW to level a character automatically
  - Blizzard claimed it infringed copyright by loading a copy into memory
  - By that reasoning, just playing the game is a violation
  - Blizzard wanted to establish that user doesn't own game, merely has a license
  - Really should be a contract claim, violation of license
  - Blizzard argued copyright gives them control over authorized uses
  - MDY, backed by Public Knowledge, others tried to argue that Section 117 protects against claims about in memory copies
  - First sale doctrine, that once a user buys, theirs do with as they see fit
  - Cited several precedents
  - Judge ruled in favor of Blizzard
  - Case still set to go to trial in September, unless they settle
  - Not likely to go well for MDY since Blizzard won summary judgement
  - Decision here is probably either to settle for less than awarded damages or appeal
  - Sets another precedent that others may be able to use
  - Erodes section 117 a bit but not widely
- Patry on Blizzard case
  - <http://williampatry.blogspot.com/2008/07/strange-copyright-world-of-warcraft.html>
  - Explains there was also a DMCA claim
  - Based on warden spyware Blizzard uses to detect cheating
  - Judge dismissed DMCA claims, at least
  - Critical of the ruling, thinks the judge really stretched to support it
- More on Blizzard ruling

## Offset

## Topic

16:21

- <http://feeds.publicknowledge.org/~r/publicknowledge-fulltext/~3/336515994/1657>
- Explains judge's interpretation of sale as license
- Points out problem in thinking that sale and license are mutually exclusive
- This is not necessarily true, example provided is owning DVD but needing license for public performance
- Points out that the danger it presents is others can craft EULAs modeled after Blizzard to eliminate section 117 protection
- Also mentions that MDY will appeal
- Android builds released under NDA, not so open
  - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/336546040/20080715-googles-android-platform-not-so-open-after-all.html>
  - New iPhone has increased awareness of alternatives
  - FSF is making much hay out of DRM on the iPhone, other concerns
  - OpenMoko has gotten some attention, though not favorable
  - UI seems nowhere near finished, too much a hobbyist device
  - Android seems like a better bet
  - Backed by Google, a company that seems to get UI, design
  - Originally committed to open standards, open development
  - Turns out a Google staffer posted a closed SDK build to the open list
  - Revealed that public development had stalled but privilege few still getting builds
  - Select developers signed NDAs to get advance builds
  - Few other details at this time
  - No information on the contents of the builds, whether any of the technology has shifted away from open source
  - Has seriously shaken the open community
  - No real response from Google, either, explaining its actions

20:09

- Another next generation P2P effort targeted at IPTV
  - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/338922629/20080718-major-eu-p2p-research-project-hopes-to-kill-traditional-tv.html>
  - Academic who has studied BitTorrent thoroughly heading team to build 4G P2P
  - Group, P2P-Next, is publicly and privately funded
  - 4G P2P is zero server, also sounds like may use network information more intelligently
  - Reminds me of Pando and stories about P4P
  - <http://arstechnica.com/news.ars/post/20080314-verizon-embraces-p4p-a-more-efficient-peer-to-peer-tech.html>
  - Another attempt to legitimize P2P and make it work well with carriers as opposed to stories of bandwidth hogs, congestion
  - Specifically working on streaming video

## Offset

## Topic

24:08

- Traditionally requires a server or cluster of servers, can bottleneck
- P2P has focused on download only, not suitable for streaming
- Lead, Pouwelse, believes P2P and streaming can be melded effectively
- One of the projects goals is to replace traditional broadcast TV
- Realistic about existing bandwidth, trying to be effective with current and future networks
- Building on existing, open source P2P client, Tribler to create new Swarmplayer
- Tribler already cross platform--Windows, Linux, OS X
- Will support traditional BT downloads as well as new streaming
- Researchers are inviting public to use trial version, help work out kinks
- Not trying to lock up the technology
- Admits pirate use is going to be a problem, doesn't say it is one the researchers will try to solve
- Pouwelse thinks research could help with peer production, distribution of open/free content like HD video for Wikimedia's work
- Recovering old software from cassette tape
  - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/335941527/article.pl>
  - Software was BASIC for the Apple I
  - That machine is rare, very few originally produced
  - Not all came with BASIC
  - Was the first commercial software Apple sold
  - Article details the recovery from tape
  - Others have done before but perhaps not with the same fidelity
  - If you are curious about analog to digital conversion, this is a great working example
  - Program was only 4KB
  - Memory location when loaded was fixed
  - Contemporary computers either loaded from cartridges, firmware, or cassette
  - Remember using Atari 400/800's at school with carts and cassettes
  - Next steps would be for assembly hackers to review
  - Important for how limited systems were used
  - BASIC was one of the first languages for many hackers of my generation and earlier
  - As an interpreted language, good for what if experimenting
  - Glad this has been recovered and will be preserved on the Internet

27:02

- **tail -f**

27:21

- EU considering extending copyright, again
  - <http://techdirt.com/articles/20080715/0101411681.shtml>
  - EU's internal market commissioner pushing for it

## Offset

## Topic

29:31

- Despite Gowers report that found extending would be harmful
- Even recommended shortening
- Also despite a past attempt in the UK that was foiled
- McCreevy seems to think copyright is a welfare system
- Wants term extend from 50 to 95 years
- Wants to focus on unknown musicians, like session players
- Was to be up for vote this past week
- EU copyright extension has a use or lost it provision
  - [http://go.theregister.com/feed/www.theregister.co.uk/2008/07/16/ec\\_copyright\\_term\\_extension/](http://go.theregister.com/feed/www.theregister.co.uk/2008/07/16/ec_copyright_term_extension/)
  - EC approved the extension
  - Seems to be a moral rights issue
  - EC sided with arguments for underpaid musicians
  - So much so they built in a reversion clause
  - If labels don't actively use music after fifty years, everts to artist
  - Not exactly public friendly
- ACTA analysis
  - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/338873723/20080718-abig-wishlist-for-a-scary-secret-anticounterfeiting-pact.html>
  - Draft recommendation was originally leaked
  - RIAA wishlist was later leaked
  - Public Knowledge, even USTR itself, have revealed more input from NGOs, others
  - RIAA wants all unauthorized exchanges criminalized, regardless of profit or intent
  - Also wants ISP filtering, though doesn't use those words
  - BSA also wants filtering, objects to EU privacy laws as interfering with copyright enforcement
  - Some from progressives
  - Objecting to DRM, use of term piracy as emotionally laden
  - Also don't think online vs. offline should make a difference in enforcement, penalties
  - Ars piece concludes with individual comment, PhD student that thinks ACTA should simply be abandoned

21:18

- **Outro**
  - Contact me
    - Email to [feedback@thecommandline.net](mailto:feedback@thecommandline.net)
    - Web site at <http://thecommandline.net/>
    - IM to [command.line@skype](mailto:command.line@skype)
    - Listener comment line is 240-949-2638
    - del.icio.us tag is "for:cmdln"
    - <http://twitter.com/cmdln>

**Offset****Topic**

- 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