

| Offset | Topic |
|----------------|--|
| 00:17 | <ul style="list-style-type: none"> ● Intro <ul style="list-style-type: none"> ● Creatively tapped out <ul style="list-style-type: none"> ● Small tech companies thrive on creative ● If you aren't growing, changing, then you are beaten by competitor who are ● Pushing out a new product next year, in the midst of that development ● Powers that be are already moving on to what features, developments are next ● I have been pulling back from work, trying to preserve a better balance ● Still don't feel like I have much energy, creativity left for myself ● Not sure what the answer is, yet, just trying to understand the problem |
| 07:14 07:34 | <ul style="list-style-type: none"> ● Security Alerts <ul style="list-style-type: none"> ● More fine grained, flexible security permissions in Linux <ul style="list-style-type: none"> ● http://www.oreillynet.com/onlamp/blog/2007/11/policykit_looser_limitations_t.html?CMP=OTC-6YE827253101&ATT=PolicyKit+looser+limitations+tighter+security+for+Linux+applications ● New tool for authorization, included in Fedora 8, PolicyKit ● Similar to Authorization Services under OS X ● Enforced by the operating system but not limited to the kernel ● A flexible framework all applications, services can use ● Allows privilege escalation, can prompt for user authentication, like Authorization Services ● Re-uses much of what is already there, e.g. PAM and HAL ● Adds notion of subject, action and target which existing components don't share ● Should make security management, use easier under Linux ● That should result in more, better security |
| 09:31 | <ul style="list-style-type: none"> ● Potential backdoor in part of new NIST PRNG standard <ul style="list-style-type: none"> ● http://www.schneier.com/blog/archives/2007/11/the_strange_sto.html ● Like AES and forthcoming AHS, NIST released PRNG standard ● Random numbers critical to security algorithms, making keys and parameters hard to guess ● Four recommended algorithms ● One, based on elliptic curves, apparently came from NSA ● Had been shown to have a small bias at time standard was published, appendix provided workaround |

Offset

Topic

- Niels Ferguson, Dan Shumow at CRYPTO 2007 showed flaw that could be seen as back door
- Basically, a set of arbitrary numbers included in EC algorithm
- Another set of numbers can be matched, act like skeleton key
- Allow attacker to predict all of the PRNG's output
- Don't know this second set of numbers
- If an attacker can discover them, though, consequences are huge
- Standard does recommend a procedure that stymies this flaw, but is optional
- No one knows why the NSA insisted on this algorithms inclusion
- Subversion seems unlikely since the standard and its works are public

14:53

• News

15:08

- Federal intelligence official begs re-definition of privacy in pursuit of wiretaps
 - <http://www.cnn.com/2007/POLITICS/11/11/terrorist.surveillance.ap/index.html>
 - Kerr argues privacy should not mean anonymity
 - Says privacy should mean corporations, government protecting private data
 - Compares government surveillance to access an ISP worker has
 - Thinks changing norms around social networking sites justifies less protection of anonymity
 - EFF correctly calls out the gap in his logic, that voluntary disclosure is not the same thing as surveillance
 - Opsahl also points out anonymity is a critical aspect of free, political speech
 - Constitution says protection from search, seizure is one of our rights
 - This in the context of NSA wiretaps, bill to legalize
 - Argument is that if one end of communications is outside US, then a weaker standard should apply
 - Foreign surveillance had such a standard, FISA court
 - The bill seems to be arguing for an even weaker standard
 - Most controversial aspect is immunizing telcos from suits for violating effective standards
 - Doesn't seem like there's a great deal of support
 - Norms cannot be changed directly
 - Congress should consider regulating market or applying other pressures, constraints
 - If they cannot reason out how to do so, then they have to work with existing norms
 - Schneier on Kerr
 - http://www.schneier.com/blog/archives/2007/11/redefining_priv.html
 - Links to transcript of the speech

Offset

Topic

21:22

- Points out that you cannot easily separate privacy, anonymity and security
- Concedes Kerr's remarks are more nuanced than credited
- Admittedly, Kerr admits t wanting to preserve privacy
- Light on what that means when he definitely wants to eliminate anonymity
- Details of OLPC mesh network
 - http://www.oreillynet.com/onlamp/blog/2007/11/mesh_networks_on_olpc_its_all_1.html
 - Focus is on application
 - Not surprisingly, OLPC is about what recipients will be able to do with meshes, not just on the technology for its own sake
 - Applications can be writing to take better advantage of network
 - Using asynchronous messaging instead of synchronous procedure calls
 - Any such message could be re-written to transparently use the network
 - Cache consistency, sharing apps have to synchronize so they have consistent local views of each other's data
 - Discovery and presence, finding each other on the network to do work
 - Implemented their own, rather than using Zeroconf
 - OLPC's discovery includes application awareness
 - Asks whether this model makes sense more generally
 - Sounds similar, actually, to the way a lot of Apple applications work
 - Leverage Zeroconf for discovery
 - More dependent on each application for discovery, but focus is on ease of collaboration
 - Mentions past issues of scaling meshes
 - Problems seem to be well solved, though
 - Mentions adoption of a similar scaling trick, super nodes, that P2P has used
 - Super nodes act as aggregators, making broadcast more efficient
 - Another perception of mesh is that centralized networks are better, mentions transition between mesh and DSL on Czech Republic
 - Received wisdom is mesh and P2P relieve strain on server but spread more load onto network itself
 - OLPC mesh work may have applicability even in developed nations, though, where ad hoc is key or gaps in traditional access
 - Has some updates, at the end, which are consistent with Paul's remarks
 - Mesh is still under very active development, many promising new ideas, implementations
- Cipher challenge with Colossus for new computing museum
 - <http://rss.slashdot.org/~r/slashdot/eqWf/~3/184268346/article.pl>

27:28

Offset

Topic

30:14

- UK's National Museum of Computing has rebuilt a Colossus
- World's first programmable digital computer
- Used at Bletchley Park during WWII to decipher German messages
- To commemorate, holding a special code breaking challenge
 - Two groups of amateur code breakers
 - Encrypted messages using period German cipher machine, transmitted from Germany and intercepted at Bletchley
 - One team will use modern PCs, the other the Colossus replica
- TNMoC also building a facility at and to preserve Bletchley
- Original machines were completely dismantled, the restoration was painstaking
- Colossus challenge won
 - http://go.theregister.com/feed/www.theregister.co.uk/2007/11/16/german_code_breaker_defeats_colossus/
 - Teams at Bletchley, Paderborn using period radio equipment, too
 - Had difficulties with interference, extended period of just trying to get messages
 - Amateur code breaker, Joachim Shcuth, in Germany intercepted, as well
 - Cracked the most heavily encrypted of the three messages, two hours before teams at Bletchley
 - Officially acknowledged by challenge coordinators at TNMoC
 - Wrote his specialist software in Ada
- Blowable interface
 - http://www.makezine.com/blog/archive/2007/11/blowable_computer_interfa.html?CMP=OTC-0D6B48984890
 - Research at GA Tech
 - Link is to a short research paper
 - Motivation was supplemental input as well as for accessibility
 - Designed around existing commodity systems, in particular laptops which typically include a single mic
 - Alternative to voice recognition, gaze tracking
 - Call their software BLUI, Blowable and Localizable User Interaction
 - Key is their processing with a single mic that can tell at which part of the screen the user is blowing
 - Previous work was simpler, detected just if user was blowing
 - Generates a generic event stream, like typical mouse drivers
 - Applications would not necessarily need to be aware of BLUI
 - Good detail in the paper but still very readable
 - Examples of interaction, not just the algorithm for localizing the blowing

33:21

- **tail -f**
 - Label chief owns up to DRM mistake
 - <http://feeds.engadget.com/~r/weblogsinc/engadget/~3/185215512/>

Offset

Topic

- Bronfman to wireless carriers
- Advised not to go to war with customers
- Admits that label's behavior in the past was unwise
- Characterizes refusal to change business model, directly address customer needs as "war"
- Points out packaging at iTunes as positive example, urges carriers to learn from iTunes
- Same person who made stink over pricing within iTunes, wanting variable per track
- Latest on Google 700MHz bid
 - <http://feeds.wired.com/~r/wired/topheadlines/~3/185976096/google-to-go-it.html>
 - Google's original interested assumed to be done with partners, other tech companies interested in spectrum
 - Now sources are saying Google will bid on its own
 - May also bid on other spectrum blocks, once not required to be open though may be limited in other ways
 - Google has apparently hired game theorists to help formulate its strategy
 - Seems pretty serious about its commitment to open wireless if some sort
 - Many are speculating this may involve Android, be a voice and data play competitive with wireless carriers

• **Outro**

- Contact me
 - Email to feedback@thecommandline.net
 - Web site at <http://thecommandline.net/>
 - IM to [command.line@skype](skype:command.line)
 - Listener comment line is 360-252-7284
 - 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