

Offset	Topic
00:17	<ul style="list-style-type: none"> • Intro
	<ul style="list-style-type: none"> • In this episode <ul style="list-style-type: none"> • A long overdue update to Debian is finally release • Debunking the myth of the superhacker • It is linux's turn for a severe and exploitable WiFi flaw • AACS is cracked again • BaltiCon 41 <ul style="list-style-type: none"> • May 25th-28th • http://balticon.org/
02:20	<ul style="list-style-type: none"> • Security Alerts
02:39	<ul style="list-style-type: none"> • DNS server flaw <ul style="list-style-type: none"> • http://go.theregister.com/feed/http://www.theregister.com/2007/04/13/windows_dns_flaw/ • Windows specific, not all version vulnerable • Normal DNS traffic is unaffected • This is a problem with Microsoft's RPC interface to their DNS server • Is a typical buffer overrun that takes advantage of DNS running essentially as root • No patch available • The simple workaround is disabling remote access to RPC • Why does Microsoft's server had RPC? • Article doesn't say how many public DNS servers are Microsoft • For large private networks, this may be more of an issue • There are plenty of DNS alternatives out there that may be more secure, certainly don't have RPC • This is like ActiveX, why add more capabilities than are needed?
05:46	<ul style="list-style-type: none"> • Linux WiFi flaw <ul style="list-style-type: none"> • http://www.techworld.com/mobility/news/index.cfm?newsID=8546&pagtype=samechan • http://www.securityfocus.com/bid/23433/discuss • Affects MadWiFi driver, for Atheros chipsets • Example of responsible disclosure and a patch from the driver team is already available • Not all distros have included the patch • When in doubt, patch manually and re-build your kernel • System doesn't have to be on a network but I imagine the transceiver has to at least be on • Discovery of exploit based on Maynor, Elch fuzzing work on other drivers
08:49	<ul style="list-style-type: none"> • News

Offset	Topic
09:03	<ul style="list-style-type: none"> • Debian Etch released <ul style="list-style-type: none"> • http://www.debian.org/News/2007/20070408 • Update to Sarge, too • 21 months of development for Etch • New, fully integrated installer • Support for encrypted partitions • Adds security features to APT • Differential update of indices • Brings most of the major packages up to date • Is this too little, too late? • Seems to have been a lot of internecine strife, lately • The features are attractive, but would have been killer a few years ago • May download and find a system to give it a whirl on, was my favorite distribution, though not my first
12:51	<ul style="list-style-type: none"> • IBM and another identity offering <ul style="list-style-type: none"> • http://go.theregister.com/feed/http://www.regdeveloper.co.uk/2007/04/09/ibm_identity_mixer/ • Identity mixer, IBM's masking technology • Dick mentioned this in the interview • First code release for the Higgins Trust Framework • http://en.wikipedia.org/wiki/Higgins_trust_framework • Next release will be an identity select, for choosing sources of data • Prototype code, only, not any kind of finished software users can use • There does appear to be a Firefox extension available • http://wiki.eclipse.org/index.php/Higgins_Browser_Extension • Higgins appears to be complementary with Microsoft's InfoCard • Project lead claims compatibility with MS and OpenID is a high priority • Links to a demo • Warns that the UI and API may be a bit more complex than users expect, justified by capabilities
17:15	<ul style="list-style-type: none"> • What does AFP settlement say about Google's stance on copyright? <ul style="list-style-type: none"> • http://www.pcworld.com/article/id,130498-c,google/article.html • Agence France Presse • This actually seems to touch on some of the same issues as library suit • Google's action enhances discovery and does not substitute for AFP's news stories • Why AFP would want to reduce or eliminate this exposure is a bit mind boggling • Article points out we don't know who caved • Some claim Google is becoming more likely to deal

Offset	Topic
20:27	<ul style="list-style-type: none"> • AFP and some news services do not benefit as much from increased exposure • Rely more on service fees than ad placement • Another expert claims the opposite • Cites similar reasons that I suggest • Also believes Google had a strong defense, if it went to trial • Why would Google settle if it opened them to others seeking payment? • Myth of the superhacker <ul style="list-style-type: none"> • http://volokh.com/posts/chain_1176127892.shtml • Concerned about invoking superhackers instead of genuine empiricism • Cites some examples in security, privacy and DRM • DRM is different because the myth is used by both sides • Explains why claims about super hackers are exaggerated <ul style="list-style-type: none"> • Statements are so hyperbolic they are self disproving • Experience suggests more common users committing cybercrimes • Studies and statistics belie the myths • Discusses harms from legislative reaction to myth <ul style="list-style-type: none"> • Overboard laws, can make simple activities into felonies • Infringements of civil liberties <ul style="list-style-type: none"> • Law enforcers feel the need in order to find these hackers • Silly to assume all criminals are equally sophisticated • Guilt by association • Wasted investigative resources • Wasted economic resources • Concludes with failure of expertise • Curious as to why security experts not as interested in stats and probabilities • Four possible explanations <ul style="list-style-type: none"> • Pervasive secrecy, think trade secret and abuse of IP law • Role of expert is dilute, too easy to attain • Self interest, using myth as a stalking horse for other ends • Need for more cooperation across disciplines, too much not my problem going on from IT to criminalist to others • Single recommendation, better data, substantiate claims, be empirical
25:44	<ul style="list-style-type: none"> • <code>tail -f</code>
26:03	<ul style="list-style-type: none"> • AACS vulnerable despite patches <ul style="list-style-type: none"> • http://go.theregister.com/feed/http://www.reghardware.co.uk/2007/04/10/aacs_hold_exposed/ • Uses Xbox 360's drive with no modification to recover volume IDs

<u>Offset</u>	<u>Topic</u>
28:42	<ul style="list-style-type: none"> • Does not authorize volume keys, so bypasses their revocation • Doesn't necessarily help copying but allows playback of copied titles • BT prefers adding bandwidth to tiered service <ul style="list-style-type: none"> • http://techdirt.com/articles/20070413/011103.shtml • Good to hear a carrier admit this • Enough detail to find the opinion credible • However, critical of FTTx
30:09	<ul style="list-style-type: none"> • Outro <ul style="list-style-type: none"> • Contact me <ul style="list-style-type: none"> • Email to feedback@thecommandline.net • Web site at http://thecommandline.net/ • IM to command.line@skype • Listener comment line is 360-252-7284 • del.icio.us tag is "for: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 <ul style="list-style-type: none"> • http://creativecommons.org/licenses/by-nc-sa/3.0/us/ • Attribution, non-commercial, share alike