

Offset	Topic
00:17	<ul style="list-style-type: none"> • Intro
02:12	<ul style="list-style-type: none"> • Security Alerts
02:31	<ul style="list-style-type: none"> • Gmail cookie stealing tool <ul style="list-style-type: none"> • http://voices.washingtonpost.com/securityfix/2008/08/new_tool_automates_cookie_stea.html • Based on a talk at DefCon • Problem is that your session cookie may be sent in the clear • This can happen even if you use https for access to Gmail • If an attacker forces a view of an image or page from Gmail in the clear, cookie gets sent in the clear • Presenter, Mike Perry, also had code to automate this attack • Other popular services are vulnerable in the same way • Problem is actually at last a year old • Google finally added a setting to Gmail to force secure cookies only • Should appear under outgoing message encoding in settings • Must use this setting, secure login is not enough as it doesn't constrain cookies to https only • Also, logging out rather than allowing these cookies to linger can help • Good advice for other sites that may be vulnerable • May not be available for domain users, other google apps yet
05:55	<ul style="list-style-type: none"> • Passwords resets less secure than re-using old passwords <ul style="list-style-type: none"> • http://www.itworld.com/tech-society/54193/beware-meta-password-reuse • Big problem is using same password for multiple sites, services • Magnifies scope, scale of someone else discover password • Users can do better, though • For common password recovery, same problem seems to occur • People use same meta information to confirm identity to invoke a reset • Sites, services constraint choices, though, usually in form of a question • Deducing answers are not hard, especially with public searches, databases • Worse, questions can be obscure, change, or difficult to answer consistently • Shares an example of a different way to go • System prompts for preferences • Psychology says preferences are mostly static • Would have liked to see a bit more on minimum preferences for confidence

Offset	Topic
09:43	<ul style="list-style-type: none"> • Seems like two choices, like and dislike, could be attacked randomly • Would have to be coupled with limits, timeouts
09:57	<ul style="list-style-type: none"> • News • EFF stepping in to defence MIT hackers against transit authority <ul style="list-style-type: none"> • http://www.infoworld.com/article/08/08/11/EFF_to_appeal_court_order_halting_subway_hacker_talk_1.html • Students were going to present at DefCon on vulnerabilities in MBTA system • Consistent with hacks in other fare card systems, like London's Oyster and DC's paper fare cards • Even heard tell of an ancient exploit in BART's old mag swipe cards, similar to the recent exploit of DC's mag strip cards • MBTA sought and won a temporary injunction • Anderson, Ryan, Chiesa presenting based on class project work • MIT also named as a defendant, probably because they knew about the material • Court cites computer crime law as basis of ruling, classifying fare system as computer • EFF disagrees, fight the injunction on the students behalf • EFF's Opsahl claims information on talks published previously in regular press • Thinks this erodes the MBTA's case and hence the reasoning behind the injunction • Slides of talk already distributed to DefCon attendees on CD, MBTA also inadvertently released further details through court records • Again, eroding the argument about disclosure critical information • Student's work look at entire system, not just the fare cards • Special focus on those, though, as a non-secure RFID application • MBTA uses Mifare cards, same vendor having problems elsewhere • MIT students response to transit authority over pulled talk <ul style="list-style-type: none"> • http://www.eff.org/deeplinks/2008/08/mit-students-response-mbta-statements • MBTA is misrepresenting the sequence of events • Trying to make out that the students were uncooperative • Students in fact contacted them first • Supplied them with plenty of information • Students, their professor Rivest thought early discussions had settled the issue • MBTA went to court before notifying students they would be doing so • Transit official supports students <ul style="list-style-type: none"> • http://www.eff.org/deeplinks/2008/08/mbta-transit-official-supports-mit-students-story • Confirms their version

- Supports that they delivered the requested information and then some
 - Also that students claimed they had never exploited the system
 - Further that they never would nor would they teach others to do so
 - Jibes with initial story, that they left key pieces out of the presentation
 - Many support MIT students
 - <http://www.groklaw.net/article.php?story=2008081309502119>
 - A group of CS professors and computer scientists support the students
 - Claim TRO should be vacate for three reasons
 - The order is unconstitutional prior restraint on the free speech
 - Computer Fraud and Abuse Act doesn't prohibit discussions of computer security
 - The publishing of info by MBTA itself erodes their claims for injunctive relief
 - Reiterates and bolsters claims of EFF
 - Prior restraint, form of censorship, prohibits students from telling their side of the story
 - MBTA is under no such restriction, spreading misinformation
 - MIT students still under gag order
 - <http://feeds.wired.com/~r/wired/topheadlines/~3/365157129/mit-students-su.html>
 - Second judge upheld original TRO
 - Considering requests for modifications from both parties
 - MBTA is seeking to get more information from students, including emails and copies of their original paper
 - EFF keeping their strategy under wraps
 - Seem to be focusing on pre-publication review, prior restraint, though
 - This is the question of responsible disclosure, but with a system non-technical people can appreciate
 - What is clear is much of the vulnerability information is already available
 - If the MBTA showed better evidence of wanting to address problems, perhaps prior restraint, non-disclosure would be warranted
 - Public discussion seems to be the only alternative in the face of unwillingness to really solve problems
 - Problems affect honest riders, raising fares, adding restrictions, limits
- Court supports open source license as conditions on copyright
 - <http://www.eff.org/deeplinks/2008/08/condition-or-covenant-and-why-should-you-care>
 - Recent activity on appeals in Jacobsen case
 - Talked about this when SFLC was suing for GPL breaches

- This is the case that had gotten the farthest in court testing an open source license
- License in question is the Artistic License, over some model railroad code
- Judge vacated a ruling that AL was just an issue of contract
- Upheld that it is a condition on a copyright
 - Governed by federal, not state law
 - Stiffer potential penalties, arguably greater protection
 - EFF article does a good job of explaining the difference
- Opinion was surprisingly broad, clueful speaking to benefits of public licenses generally
- Unfortunately, supporting conditions on copyright opens abuses in EULAs, too
- Those could be contested, tested separately though
- GrokLaw on Jacobsen case
 - <http://www.groklaw.net/article.php?story=20080814141638469>
 - Basically, she thinks licenses now care more weight, for good and ill
 - Time to involve more legal experts both in crafting and choosing licenses
- PK on Jacobsen case
 - <http://feeds.publicknowledge.org/~r/publicknowledge-fulltext/~3/366044421/1712>
 - Points out the key difference between open source and EULA conditions
 - EULA typically conditions just use
 - Uses Blizzard v. MDY as an example, EULA governs use of game, service
 - Open licenses govern copyright actions, copy, remix and distribute
- Using CAPTCHAs to help scanning texts
 - <http://feeds.arstechnica.com/~r/arstechnica/BAaf/~3/364993719/20080814-captchas-workfor-digitizing-old-damaged-texts-manuscripts.html>
 - Starts describing one archival problem
 - Texts most often in need of digital preservation are already damaged
 - Makes them that much harder for an imperfect technology to handle
 - CMU researchers saw similarities between digitization problem, CAPTCHAs
 - Launched a project a year ago to turn problem text into CAPTCHAs
 - Called reCAPTCHA
 - Get humans to help recover damaged text
 - Have just shared their results
 - Had over 40K sites participate
 - Use control words to help weed out spam bots

- Also have multiple human guesses per word, weighting improves accuracy
- Tested with 250 NYT articles from different eras
- Already had reliable transcriptions
- OCR alone achieve 84% or so, with reCAPTCHA, went up to 99.1%
- Comparable to professional, expert human services
- Turns out reCAPTCHA images are also more resistant to machine attacks
- Guess that is a result of them not being generated by smooth math transforms
- Time for real users to guess also not significantly different from traditional CAPTCHAs
- Some issues with sites in non-English speaking countries or ESL
- An intangible social benefit, too, that users like that they are contributing to a larger project
- There is an API and a PHP library if you are interested in using
- <http://recaptcha.net/>
- Renewed push for next version of JavaScript
 - http://feeds.wired.com/~r/wired/topheadlines/~3/365104855/JavaScript_2_Looking_Good_Thanks_to_Harmony_Project
 - Talked about Eich's thoughts on ECMAScript 4.0/JavaScript 2
 - Microsoft and Yahoo balked at ambitions of 4/2
 - Split off to work on ECMAScript 3.1, as a practical step towards 4
 - Two groups have reached an accord
 - Agreed on project for release, Harmony
 - Among other things, drops packages and namespaces
 - Looks like these, along with early binding, dropped permanently
 - Harmony focusing on release next year and plans beyond
 - Article points out also affects Adobe's ActionScript
 - May also place Tamarin, Screaming Monkey in jeopardy
 - I am concerned that packages are completely gone
 - I don't think JavaScript intensive applications will scale well without
 - I doubt that web applications are going to stop getting larger, more complex
 - Already have several competing libraries, how to handle when there are inevitable collisions?
 - Libraries aren't completely interchangeable so foolish to suggest using just one
 - More concerned that Microsoft derailed this effort
 - The web continues to be fractured by them even as more and more applications move into the cloud with web interfaces
 - Despite seeming consensus on 3.1, how compatible will their implementation really be?

Offset	Topic
29:32	<ul style="list-style-type: none"> JavaScript is also only part of the picture, if their rendering, object model and style support continues to be different, just as bad as ever
29:51	<ul style="list-style-type: none"> tail -f
29:51	<ul style="list-style-type: none"> Pandora about to close up shop <ul style="list-style-type: none"> http://www.readwriteweb.com/archives/pandora_on_the_verge_of_closing_shop.php I have raved about Pandora before Uses music genome project, database of traits of music for identifying similarities Has come under fire abroad Forced by license costs, inability to negotiate licenses to close shop anywhere but the US Company is now facing a decision to shut down altogether This is a long range consequence of web royalty hike from last year Read somewhere that Pandora pays a huge chunk of its revenue to SoundExchange Company is hoping Rep. Berman can negotiate a more sane rate They are not optimistic
31:17	<ul style="list-style-type: none"> RIAA pays Andersen's legal fees <ul style="list-style-type: none"> http://rss.slashdot.org/~r/slashdot/eqWf/~3/365655967/article.pl Not only did she win in the labels' case against her She has been paid Not just the judges order, court creditors have confirmed labels paid over 100K in lawyers fees plus interest May encourage others to fight back, it is possible While she hasn't recovered any damages, she also doesn't have to cover her own fees Has already launched a counter suit for malicious prosecution Andersen v. Atlantic could settle the questions over investigatory practices Whether agents are legal to investigate where and how they do Question of wether downloads by investigators is sufficient evidence or constitutes an authorized use
33:27	<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 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

Offset**Topic**

- 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