Security Cannot Be Spun

By John Gruber

Perhaps the most surprising aspect of the recently-publicized Mac OS X security vulnerabilities has been the press coverage. Compared to the sensationalized and misleading coverage that appeared a month ago about Intego's "MP3Concept Trojan Horse" scam, the response to the current URI-related vulnerabilities has been, well, measured and appropriate.

If anything, the coverage has been *underplayed*. These are serious vulnerabilities which could be exploited for serious harm. You could reasonably argue that this is the worst security problem in the entire history of the Macintosh. And if it's not *the* worst vulnerability, it's certain up there.

That's the bad news.

At this point, it's worth noting the difference between a *vulnerability* and an *exploit*. A vulnerability is a security hole; an exploit is an action that takes advantage of a vulnerability. An unlocked car door is a vulnerability; when a thief opens the unlocked door and steals the car, that's an exploit.

To date, all of Mac OS X's URI-related security problems are mere vulnerabilities—there are no publicized exploits (other than innocuous proof-of-concept examples).

That's the good news.

The fact remains that the overall state of security on Mac OS X is very good. It's not as good as we thought it was two weeks ago, but that doesn't mean it isn't excellent overall. This might strike you as an odd thing for a Mac user to gloat about in light of the recently-publicized vulnerabilities, but it's true.

But this is where non-technical Mac enthusiasts often go overboard, e.g. by bragging that Mac OS X "has no vulnerabilities", or that it "can't be hacked", etc. Such claims make no sense. What does make sense, and is true, is that Mac OS X has had relatively few vulnerabilities exposed, and that when they have been publicized, Apple has closed them in reasonably short order.

It'd be nice, however, if I could have used the word *identified* rather than *publicized* in that last sentence. But I can't, because the worst aspect of these security issues hasn't been the vulnerabilities themselves, but Apple's response to them.

It ends up that Apple was notified about the Help Viewer 'help:runscript' URI vulnerability by someone named "Lixlpixel" on February 23, but as far as can be determined by anyone outside the company, Apple did nothing in response until last week, when the vulnerability was made public and garnered significant attention.

WHY 10.3.4 DOESN'T FIX THE REMAINING VULNERABILITIES

Ostensibly, Lixlpixel did the right thing, or at least did what Apple would prefer people do when serious vulnerabilities are identified. Ideally, notifying Apple privately would engender the same response as publicizing the vulnerability in the press.

But, alas, apparently not. "Sweep them under the rug" is not a serious security policy, and the IT press is taking notice. E.g. "Apple releases latest Mac [*sic*] version—with holes left in" by Kieren McCarthy in Techworld.

McCarthy takes Apple to task for two things:

1. Mac OS X 10.3.4 does *not* encompass Security Update 2004-05-24. Indeed, this seems odd, given that (a) the security update was released prior to Mac OS X 10.3.4, and (b) 10.3.4's release notes claim that it "Includes recent Mac OS X Security Updates."

2. Even after installing both Mac OS X 10.3.4 and Security Update 2004-05-24, the Launch Services/URI-related security vulnerabilities are not addressed. This seems odd, given the severity of the vulnerability and the amount of publicity it has received.

But in fact, although both #1 and #2 are true, neither is particularly odd.

Take #1—updates which bump the version number of the entire OS are a big deal, and are in the works for a relatively long period of time. Work on 10.3.4 probably commenced even before 10.3.3 shipped back in March. More importantly, OS updates are rigorously tested before release. Security Update 2004-05-24 for Panther was quite small: all it contained was an updated version of Help Viewer. But that doesn't mean Apple could have just thrown it into the 10.3.4 update at the last moment. Adding new software to the 10.3.4 update would have required restarting the testing process for the entire update. The "add new features and fixes to the update" period probably closed weeks ago. I.e., Mac OS X 10.3.4 was almost certainly slated for release long before these vulnerabilities came to light. The timing is merely coincidence.

You can't argue that Apple shouldn't have released 10.3.4 when it did. It was ready to go, and contains numerous bug fixes and improvements.

Nor does it make sense to argue that Apple should have included a fix for the remaining URI/Launch Services vulnerabilities in 10.3.4. These vulnerabilities are not caused by a bug; they're the result of an unfortunate confluence of seemingly unrelated features. A proper solution is going to require:

1. Design—finding a solution that closes the vulnerability but does not eliminate features that applications depend on.
2. Engineering.
3. Localization (Mac OS X supports many languages).
4. Testing.

Many of the same people who are irrationally complaining that Apple hasn't responded to these vulnerabilities by rushing a fix out the door are the same people who've complained in the past that Apple doesn't thoroughly test its software updates. Remember the iTunes 2 installer, which had a bug that could wipe out entire drive partitions? You can't have it both ways, folks.

Just because the vulnerability is critical doesn't change the amount of time it takes to put together a good and properly-tested solution.

COMMUNICATION BREAKDOWN

This is not to absolve Apple. But if we're going to place blame, we ought to place it precisely. Let's break Apple's responsibilities—as Mac OS X's platform vendor—into two areas:

- Design/Implementation
- Response/Communication

Design/Implementation regards the security of Mac OS X, as it stands today. Appropriate questions are, e.g., Has Mac OS X been designed with security in mind? and How secure is Mac OS X today?

Response/Communication regards the way Apple deals with security issues on an ongoing basis. Appropriate questions are, e.g., How quickly does Apple respond to new

security issues? and What kind of information does Apple provide regarding Mac OS X security fixes and issues?

The first thing to note about these distinctions is that the first area—Design/Implementation—is really about Mac OS X, the product; whereas the second—Response/Communication—is really about Apple, the company. The clueless and/or feeble-minded often conflate the two (c.f. Crazy Apple Rumors' classic "Guy About Had It With People Who Confuse 'Apple', 'Mac'."). In this case, the distinction is essential.

The second thing to note is that Mac OS X scores quite well by any reasonable standard with regard to its Design/Implementation; Apple on the other hand, scores poorly with regard to Response/Communication.

The major problem that's been laid bare over the course of the last two weeks is not that Mac OS X has major design flaws, or that it's about to be run over with serious security exploits. The problem is that Apple has been revealed as a company that treats security vulnerabilities as marketing problems, rather than as technical problems.

This is not a revelation. Serious technical publications—notably MDJ—have long been hounding Apple about its pathological reticence with regard to documenting security fixes. Here's an example from this week:

The recently-publicized 'telnet:' vulnerability was fixed with an updated version of Terminal (version 1.4.2) included with the Mac OS X 10.3.4 update. (The version of Terminal in 10.3.3 was 1.4.1.) You'd never know this by reading Apple's Security Update documentation, however, where the fix is apparently described thusly:

> **Terminal:** Improves the handling of URLs. Credit to René Puls [...] for reporting this issue.

I say "apparently" because it's impossible to determine with certainty, based on this absurdly vague description, what problem has been addressed. Somehow I doubt that Mr. Puls wrote a report stating nothing more than, "Dear Apple, I have discovered a security issue in which Terminal needs improved URL handling. Thanks."

The best we can do is guess. I've verified that the 'telnet:' file-overwriting vulnerability is closed on 10.3.4 by trying it myself. And the above item is the only issue mentioned in the 10.3.4 security update release notes that could possibly apply. But it's still a guess—for all we know, Mr. Puls's report was about some *other* URL-related "improvement" for Terminal.

These descriptions are important, because they allow serious users to make informed decisions regarding updates. Imagine you're the administrator for a network of Macs in a creative agency. Upon the release of Mac OS X 10.3.4, you need to determine when (or if) to apply the upgrade to the Macs you're responsible for. A security fix for Terminal described as "Improves the handling of URLs" not only doesn't help, it *hurts*. A reasonable Mac admin for a creative agency—whose artists likely never even launch Terminal—is not going to be concerned about "improved URL handling".

Whereas if Apple described the issue accurately—that it closes a vulnerability that allowed any remote web site to overwrite files simply by sending a 'telnet:' protocol URI—well, that's a fix you might want to roll out as soon as possible.

Thus, Design/Implementation-wise, Mac OS X 10.3.4 (combined with Security Update 2004-05-24) is fine. It fixes bugs and resolves security issues. The only vulnerabilities which haven't yet been resolved were discovered too recently for inclusion in these updates.

Response/Communication-wise, however, it's been abysmal. One of the critical security issues—the Help Viewer exploit—was reported in February, privately, but apparently wasn't acted upon until May, after it was publicized. Another critical bug—the 'telnet:' URI vulnerability—was fixed in 10.3.4, but the description of the fix was so vague that many Mac nerds didn't even realize 10.3.4 contained a fix for the issue.

Apple's upper management might want everyone to apply all software updates as soon as they come out, no questions asked, but that's not how responsible computer experts work. Faith in Apple's updates requires trust, but trust is a function of both Design/Implementation *and* Response/Communication.

Trust but verify is good advice; Apple's euphemistic approach to documenting security updates makes verification difficult at best, and in some cases, impossible. It's frustrating, because Apple knows what's been fixed, but they're just not saying.

SECURITY UPDATES ARE NOT A MARKETING PROBLEM

In response to the significant publicity the Help Viewer vulnerability garnered, Apple issued a press statement—"Mac OS X Update Addresses Security Concern"—upon the release of Security Update 2004-05-24. (Most Mac OS X security updates are not accompanied by press releases.) This PR typifies Apple's marketing-slanted approach to communicating about security updates.

Start with the obvious. The only person quoted in the PR is Phil Schiller, who, of course, is "Apple's senior vice president of Worldwide Product Marketing". Security experts and Mac IT professionals don't want to hear from marketing executives; they want to hear from engineering executives.

Then there's the content of the PR itself. Off on the wrong foot in the first sentence:

> Apple today posted a Mac OS X update to address a theoretical vulnerability in the Help Viewer application that could have been exposed when browsing the web.

This vulnerability was "theoretical" in the same sense that gravity is theoretical. It'd be fair for Apple to note that the vulnerability had not been exploited for harm, but that doesn't make the vulnerability any less real.

Next is the first quote from Schiller:

> "Apple takes security very seriously and works quickly to address potential threats as we learn of them—in this case, before there was any actual risk to our customers."

This is flat-out false. Apple's customers *were* at risk—and anyone who hasn't yet installed the security update (or manually reassigned the 'help:' URI to something other than Help Viewer) is still at risk. Apple could truthfully claim to have shipped the security update before any known harmful exploits for this vulnerability appeared, but that's not what Schiller said.

Second, given that Lixlpixel reported the Help Viewer "help:runscript' vulnerability in February, the idea that Apple "works quickly to address potential threats as [they] learn of them" deserves a raised eyebrow. What the Help Viewer saga indicates is that Apple works quickly to address potential threats only after they've been publicized, not when they've been identified and reported to Apple privately. I'm not saying that's true—it's possible that Lixlpixel's report was too vague, or that it really did take three months to fix, or that it was simply an aberration—but that's the perception.

Saying Apple "takes security very seriously" is meaningless. Judging by Apple's actions, they do not.

Schiller continues:

> "While no operating system can be completely immune from all security issues, Mac OS X's UNIX-based architecture has so far turned out to be much better than most."

For all of Apple's security-related hemming and hawing, this particular statement is pretty hard to argue with. But this is a statement about Design/Implementation, which no one is arguing about. It's Apple's Response/Communication that's a problem, and which Apple continues to exacerbate with its use of euphemistic language.

Mac OS X's security architecture *is* better than that of most other platforms. And no reasonable person would argue that any system could be "completely immune from all security issues". Thus, Apple does not need to *spin* security issues as they appear; they simple need to address them head-on, with plain language and the straight truth.

MAKING MATTERS WORSE

If the purpose of Apple's spin-control approach to addressing security issues is to improve the perception of Mac OS X, it not only isn't working—it's backfiring. Due to the aforementioned "Apple"/"Mac" conflation, criticism of Apple is often interpreted, or even directed, as criticism of Mac OS X.

Let's go back to Kieren McCarthy's scathing article in Techworld. All of the criticism in this article is effectively directed at Apple (i.e. Response/Communication), but the typical reader could easily be left with the impression that there are serious, ongoing security problems with Mac OS X (i.e. Design/Implementation).

Regarding the fact that 10.3.4 does not include the updated Help Viewer from Security Update 2004-05-24, McCarthy writes:

> This is despite Apple's stated claim that the latest version: "Includes recent Mac OS X Security Updates." On the OS' official security page, Apple claims that Mac OS X 10.3.4 is "safe and secure". "Because it's built on Open Source standards, Mac OS X provides you with time-tested security and reliability not available on proprietary systems." Its documentation also claims that security is at the core of the operating system.
>
> However, not only does a patch rated "extremely critical" not come with the latest OS but Apple makes no mention of the need to download and install it. In fact, it claims it is already installed.

Now, if you note Apple's precise language, they actually claim no such thing. "Includes recent Mac OS X Security Updates" does not mean the same thing as "Includes *all* recent Mac OS X Security Updates".

But regardless if the statement can be defended as technically (or should I say "theoretically"?) true, it's undeniably misleading. Especially given the amount of publicity it garnered just a few days before 10.3.4 shipped, it's easy to see how a reasonable person would assume that "recent Mac OS X Security Updates" would include the one recent security update that everyone is talking about.

The truth would not have hurt. As conjectured earlier, it's almost certainly the case that Mac OS X 10.3.4 was done and in testing by the time Security Update 2004-05-24 was issued. It was simply too late for inclusion. A simple, explicit note that you still needed Security Update 2004-05-24 *in addition* to 10.3.4 is all it would have taken.

With regard to the remaining URI/Launch Services vulnerabilities, McCarthy writes:

> Nonetheless, all Apple has produced by way of explanation is a short statement which reads: "Apple takes security very seriously and works quickly to address potential threats as we learn of them."
>
> Such apparent pomposity will do nothing to quell security companies' criticism of Apple. Head of Secunia, Niels Henrik Rasmussen, told us earlier this week: "Microsoft and most Linux distributions have learned the lesson and properly describe the nature and the impact of (most) vulnerabilities,

> allowing their customers to properly estimate the severity of a fixed issue. This is not possible when reading an Apple update."

Replace "security companies" with "Fortune 500 corporations", and you can see how the perception that Apple is not serious about security is costing them. It doesn't matter whether it's true or not; it's the perception that matters.

The entire negative slant to McCarthy's article—which is mirrored in other technical press coverage of the 10.3.4 update—could have been avoided if Apple had simply stated the straight truth.