



STRAIGHT DOPE ON THE VULNERABILITY DU JOUR FROM IBM Internet Security Systems

CURRENT THREAT LEVEL

[« Excel exploit \(MS08-014\) in the wild](#) | [Home](#) | [The Cost of Networking @ Blackhat](#) »



BROWSE ARCHIVES

-- Browse by Month --

LINKS

- [About Frequency X](#)
- [Contact Us](#)
- [X-Force Web Site](#)
- [Vulnerability Disclosure Guidelines](#)
- [Subscribe to Frequency X](#)

Apple Crumble @ Blackhat

Posted by **Gunter Ollmann** on March 28, 2008 at 7:08 AM EDT.

It's been an interesting day at Blackhat Amsterdam. As conference venues go, you can't really beat having Blackhat in Amsterdam - the city is alive at night (even if you manage to filter out the red hue around certain districts) - meanwhile, at the conference level, the actual number of attendees is pretty small, but the atmosphere is cozy and open to discussion; something not so common at other cookie-cutter security conferences.

The highlight of the day was the presentation given by Stefan Frei and Bernard Tellenback titled "[0-day Patch – Exposing Vendors \(In\)Security Performance](#)" covering their analysis of several years of vulnerability disclosures and patching processes from various vendors, and a detailed dissection of Apple's and Microsoft's performance. (from the X-Force perspective, we've looked this data in the past, however their analysis focused on correlating multiple external data sources and honing in on the CVE-numbered vulnerabilities with full 'cradle-to-grave' disclosure histories)

In essence, with their "0-day Patch" metrics, they managed to show just how far Apple is trailing Microsoft in security patch responsiveness – in fact, after inspecting their graphs, Apple appears to be trending entirely in the wrong direction; more vulnerabilities, longer patching times, more 0-days, etc. – not the sort of thing we expect from a well known software vendor.

While I think that there are quite a few reasons why this is probably so, I'd be inclined to say that Apple's biggest problem appears to be that they treat every new vulnerability as a potential PR disaster rather than an opportunity to visibly reinforce their work in securing their customers. In recent times this has most critically been reflected in the way Apple works with security researchers (e.g. I'm yet to find a single security researcher that has had any positive things to say about their dealings with Apple's security team).

While all of today's presentations were good and of a high quality, perhaps the most interesting presentation for me personally today was that of Christopher Tarnovsky - "Security Failures in Secure Devices".

Diving deeply in to an area of security research and vulnerability discovery that I've never been involved with, he covered his work in the field of Integrated Circuit (IC) design. It was great to see and hear of his experiences in hacking IC's – decapsulating the chip substrate, invasive probing, methods of introducing electrical and optical glitches, and generally bypassing current chip-level protection schemes.

Seeing a master like Chris discussing his work was fantastic (I guess playing with acid, lasers, and high-powered microscopes has its attractions too), and I'm sure he made it look much easier than it really is. That said, his work clearly shows that no matter how well you engineer protection (even at the chip-level), if you have unrestricted physical access to the technology you'll always be able to break it and – in this case – extract the carefully guarded cryptographic keys that lay at the heart of modern access control technologies.



©2007 IBM Internet Security Systems. All rights reserved worldwide.

[Terms Of Use](#) | [Privacy Policy](#) | [Code Of Conduct](#) | [Trademarks](#) | [Contact Us](#)

Comments or opinions expressed on this Weblog are the opinions of the authors alone. They are not necessarily reviewed in advance by anyone but the individual authors, and neither IBM Internet Security Systems nor any other party necessarily agrees with them. The views expressed by outside contributors and links to outside websites do not represent the views of IBM Internet Security Systems, its management or employees. All content on this Weblog has been made available on an "as-is" basis, and IBM Internet Security Systems shall not be liable for any direct or indirect damages arising out of use of this Weblog.