

Vista gaat gebruik documenten wijzigen!

Contributed by Administrator
Wednesday, 06 December 2006

Vista gaat gebruik documenten wijzigen! Let goed op: binnen nu en 2 jaar gaan er aanzienlijke wijzigingen optreden in het gebruik van allerlei documenten door het gebruik van de "Trusted Computing Module" (TCM) in uw systeem, Information Rights Management (IRM) en de wijze waarop Microsoft daar ge-/misbruik van maakt / gaat maken. Een bijzonder goed artikel!!!

How Vista Lets Microsoft Lock Users
In

Technology called "Information Rights Management," combined with copyright law and Windows Vista, give Microsoft the tools to hold users' data hostage in Office, says Cory Doctorow.

By Cory Doctorow

InformationWeek

Dec 5, 2006 08:19 PM

What if you could rig it so that competing with your flagship product was against the law? Under 1998's Digital Millennium Copyright Act, breaking an anti-copying system is illegal, even if you're breaking it for a legal reason. For example, it's against the law to compete head-on with the iPod by making a device that plays Apple's proprietary music, or by making an iPod add-on that plays your own proprietary music. Nice deal for Apple.

Microsoft gets the same deal, courtesy of something called "Information Rights Management," a use-restriction system for Office files, such as Word documents, PowerPoint presentations, and Excel spreadsheets.

We've had access control for documents for years, through traditional cryptography. Using PGP or a similar product, you can encrypt your files so that only people who have the keys can read them.

But Information Rights Management (IRM), first introduced in Office 2003, goes further -- it doesn't just control who can open the document, it also controls what they can do with it afterwards. Crypto is like an ATM that only lets you get money after you authenticate yourself with your card and PIN. IRM is like some kind of nefarious goon hired by the bank to follow you around after you get your money out, controlling how you spend it.

With IRM, an Office user can specify whether her documents can be printed, saved, edited, forwarded -- she can even revoke access to the documents after sending them out, blocking leaks after they occur. Documents travel with XML expressions explaining how they can and can't be used.

Now, if anyone was allowed to make a document reader, it would be simple to make a reader that ignores the rules. This is a perennial problem for Adobe's password-restricted PDFs -- the only thing that distinguishes them from normal PDFs is a bit that says, "I am a restricted PDF." Just make a PDF reader that ignores the bit and you've defeated the "security." It's about as secure as one of those bogus "Confidentiality notices" that your mail-server pastes in at the bottom of every email you send.

There are plenty of readers for Microsoft's Office formats these days. Apple makes at least two -- Pages and TextEditor. Google and RIM both have Office readers they use to convert Office documents to other formats. And there's also free readers like OpenOffice.org, which are open source and so can be modified by anyone with the interest to write or commission new code for them.

But now that the format is well understood, Microsoft needs another way to ensure that it only hands keys out to readers that can be trusted to follow the rules that accompany them. Pages or OpenOffice.org can request a set of document keys just as readily as Office can. Microsoft can try to create secret handshakes to make sure it only gives out the keys to authorized parties, but just as the document format can be cracked, so can the handshaking.

IRM has an answer. Unlike a crippled PDF, a restricted Word file is encrypted. Only authorized readers will get the keys. This technology will return Office users to the days before the file format had been

reverse-engineered by competing products like WordPerfect, where reading an Office file meant licensing the file-format from Microsoft.

If anyone makes a client that listens to its owner instead of Microsoft, then the system collapses. No-print, no-forward, revoke and other flags for the document can simply be ignored. Once Microsoft sends a decryption key to an untrusted party, all bets are off -- Microsoft loses its lock-in and you lose any notional security benefits from IRM.

This has been a purely theoretical problem until recently -- but the advent of Vista and Trusted Computing should put it front-and-square on your radar.

Microsoft has an industrial-strength answer to the problem of figuring out whether a remote client is authorized to request keys. Trusted Computing. For years now, most PC manufacturers have been shipping machines with an inactive "Trusted Computing Module" on the motherboard. These modules can be used to sign the BIOS, bootloader, operating system, and application, producing an "attestation" about the precise configuration of a PC. If your PC doesn't pass muster -- because you're running a third-party document reader, or a modified OS, or an OS inside a virtual machine -- then you don't get any keys.

What this means is that Apple can make Pages, Google can make its Doc-converter, and OpenOffice.org can make its interoperable products, but none of these will be able to get the keys necessary to read "protected" documents unless they're on the white-list of "trusted" clients.

What's more, adding crypto to the mix takes us into another realm: the realm of copyright law. The same copyright law that prohibits competing head on with Apple also prohibits competing head-on with IRM. EDI and other middleware companies built their fortunes on writing software that unlocks your data from Vendor A's format so you can use it with Vendor B's product. But once Vendor A's data-store is encrypted, you run afoul of the law merely by figuring out how to read it without permission.

Vista is the first operating system to begin to use the features of the Trusted Computing Module, though for now, Microsoft is eschewing the use of "Remote Attestation" where software is verified over a network (they've made no promise about doing this forever, of course). No company has spent more time and money on preventing its competitors from reading its documents: remember the fight at the Massachusetts state-house over the proposal to require that government documents be kept in

open file-formats?

The deck is stacked against open file formats. Risk-averse enterprises love the idea of revocable documents -- HIPPA compliance, for example, is made infinitely simpler if any health record that leaks out of the hospital can simply have its "read privileges" revoked. This won't keep patients safer.

As Don Marti

says, "Bill Gates pitch[ed] DRM

using the example of an HIV test result, which is literally one bit of information. If you hired someone untrustworthy enough to leak that but unable to remember it, you don't need DRM, you need to fix your hiring process."

But it will go a long way towards satisfying picky compliance officers. Look for mail-server advertising that implies that unless you buy some fancy product that auto-converts plain Office documents to "revocable" ones, you're being negligent.

No one ever opts for "less security." Naive users will pull the "security" slider in Office all the way over the right. It's an attractive nuisance, begging to be abused.

The Trusted Computing Module has sat silently on the motherboard for years now. Adding Vista and IRM to it is takes it from egg to larva, and turning on remote attestation in a year or two, once everyone is on next-generation Office, will bring the larva to adulthood, complete with venomous stinger.

Cory Doctorow is co-editor of the Boing Boing blog, as well as a journalist, Internet activist, and science-fiction writer.