NOT-SO-TRUSTED COMPUTING: GERMAN GOVERNMENT WORRIED ABOUT WINDOWS 8 RISKS

Microsoft’s “trusted computing platform.”

Microsoft’s “secure boot” technology.

The doublespeak almost writes itself these days. Whose “trusted computing”? Whose “platform”? And whose “secure boot”?

At least one government has expressed concerns in internal documents, buttressed by an unusual public statement in response to reports about the leaked documents.

According to German news outlet Die Zeit, internal documents from the Bundesamt fur Sicherheit in der Informationstechnik (Germany’s Federal Office for information Security – BSI) warn that Microsoft Windows 8’s Trusted Computing Platform poses a security risk.

The BSI issued a response, the first paragraph of which acknowledges the news reports; it also refers to an internal paper by the Bundeswirtschaftsministeriums (Germany’s Federal Ministry of Economics and Technology – BMWi) advising caution in using the Trusted Computing Platform. This may not be the first cautionary communication by the BMWi as it is not clear whether the paper referenced by the BSI today is the same internal paper issued on the subject in early 2012.

In the second paragraph, BSI denies it has issued any warning to private or public sector users, though this announcement doesn’t deny a warning might be warranted since government agencies are warning each other internally.

The third paragraph says that the Win 8 TCP

(using Trusted Platform Module TPM 2.0) might offer improved security for some groups, though transparency should be offered by the manufacturer.

But the kicker is the fourth paragraph:

> "From the BSI's perspective, the use of Windows 8 combined with TPM 2.0 is accompanied by a loss of control over the operating system and the hardware used. As a result, new risks arise for the user, especially for the federal government and for those providing critical infrastructure. In particular, on hardware running Windows 8 that employs TPM 2.0, unintentional errors of hardware or the operating system, but also errors made by the owner of the IT system, could create conditions that prevent further operation of the system. This can even lead to both the operating system and the hardware employed becoming permanently unusable. Such a situation would not be acceptable for either the federal authorities or for other users. In addition, the newly-established mechanisms can also be used for sabotage by third parties. These risks must to be addressed."[1]

"Loss of control over the operating system" isn't a minor trifle. This suggests that any and all computers with this "feature" could go rogue and operate in contravention to the owners' instructions, at the direction of some unseen entity on a network or by injection of an application through thumb drive, disk drive, CD, etc.

This also suggests that a Win 8 system using TPM 2.0 might well reject any attempts to use an alternative operating system – a so-called "secure boot" might cut off any application other than Win 8. For all intents and purposes, a machine with Win 8 and TPM 2.0 will operate to Microsoft's orders and to the orders of whomever

is ordering Microsoft these days. It’s not out of the question that Win 8 systems lacking valid TPM 2.0 might be prevented from accessing the internet or any other network.

Which begs the question: if Windows 8 and TPM 2.0 are installed, whose computer is it?

One of the security risks is exposure to the U.S. National Security Agency’s monitoring programs; yet another risk is the possibility of Stuxnet-like software injections, keeping in mind that Microsoft’s vulnerabilities enabled Stuxnet’s design. BSI does not mention the NSA, but the statement issued is in direct response to media reporting in which Win 8 TPM 2.0 is cited as a backdoor for the NSA.

Yet one more risk is the possibility of exposure to Chinese intelligence; cryptographic expert Professor Rüdiger Weis of Beuth University of Technology in Berlin, noted that all TPM manufacturing resides in China.

The Trusted Computing Platform – originally developed in concert with other technology firms through the Trusted Computing Group – and Microsoft’s Windows Genuine Advantage technology have been questionable all along. What once looked like legitimate verification of legally licensed applications, updates of firmware and driver software, and the ability to push security patches once a month or on an urgent, as-needed basis now looks like a vector for pushing NSA monitoring scripts, among other possibilities.

What information security entities have been checking line-by-line through Microsoft’s monthly Patch Tuesday code for intelligence gathering content? How many users ever bother to ask about the validity of patches, updates, or upgrades, including those which demand driver updates on non-Microsoft peripheral devices? How many users simply accept default settings in any Microsoft application because doing otherwise is a complicated headache, or sets their system up for an application conflict?

Microsoft and in turn the NSA have relied on the inconvenience of questioning anything but default ubiquity to ensure propagation of their technology. With the use of Win 8 TPM 2.0 as a standard for manufacturing, both Microsoft and the NSA may be assured systemic compliance based on unified conformity.

There’s one more avenue for systemic compliance with Win 8 TPM 2.0, as noted in the recent rejiggering of Microsoft’s business structure. With all hardware platforms now reporting to a single Windows manager, all systems will conform to the same standard – all personal computers, netbooks, tablets, and cell phones running the same operating system.

The only questions remaining: when will Microsoft’s Xbox platform migrate to the same Windows standard with regard to TPM 2.0, and how long thereafter will it take the gaming community to begin to walk away from Xbox.

[1] Translated paragraph via Glyn Moody at ComputerworldUK.