



"Die Vorteile von Notebooks für mittelständische Unternehmen".  
Hier klicken und lesen.


▼ new issue  
terminal

search subscribe forum imprint




## How NSA access was built into Windows

*Duncan Campbell* 04.09.1999

Careless mistake reveals subversion of Windows by NSA.

 download

A CARELESS mistake by Microsoft programmers has revealed that special access codes prepared by the US National Security Agency have been secretly built into Windows. The NSA access system is built into every version of the Windows operating system now in use, except early releases of Windows 95 (and its predecessors). The discovery comes close on the heels of the revelations earlier this year that another US software giant, Lotus, had built an NSA "help information"  [trapdoor](#) into its Notes system, and that security functions on other software systems had been deliberately crippled.

[no-flash version](#)

 related stories

[Only NSA can listen, so that's OK](#)

The first discovery of the new NSA access system was made two years ago by British researcher Dr Nicko van Someren. But it was only a few weeks ago when a second researcher rediscovered the access system. With it, he found the evidence linking it to NSA.

Computer security specialists have been aware for two years that unusual features are contained inside a standard Windows software "driver" used for security and encryption functions. The driver, called ADVAPI.DLL, enables and controls a range of security functions. If you use Windows, you will find it in the C:\Windows\system directory of your computer.

allows Microsoft to export. That information is bad enough news, from a European point of view. Now, it turns out that ADVAPI will run special programmes inserted and controlled by NSA. As yet, no-one knows what these programmes are, or what they do.

Dr Nicko van Someren reported at last year's Crypto 98 conference that he had disassembled the ADVADPI driver. He found it

contained two different keys. One was used by Microsoft to control the cryptographic functions enabled in Windows, in compliance with US export regulations. But the reason for building in a second key, or who owned it, remained a mystery.

## A second key

Two weeks ago, a US security company came up with conclusive evidence that the second key belongs to NSA. Like Dr van Someren, Andrew Fernandez, chief scientist with Cryptonym of Morrisville, North Carolina, had been probing the presence and significance of the two keys. Then he checked the latest Service Pack release for Windows NT4, [Service Pack 5](#). He found that Microsoft's developers had failed to remove or "strip" the debugging symbols used to test this software before they released it. Inside the code were the labels for the two keys. One was called "KEY". The other was called "NSAKEY".

Fernandes reported his re-discovery of the two CAPI keys, and their secret meaning, to "Advances in Cryptology, Crypto'99" conference held in Santa Barbara. According to those present at the conference, Windows developers attending the conference did not deny that the "NSA" key was built into their software. But they refused to talk about what the key did, or why it had been put there without users' knowledge.

## A third key?!

But according to two witnesses attending the conference, even Microsoft's top crypto programmers were astonished to learn that the version of ADVAPI.DLL shipping with Windows 2000 contains not two, but three keys. Brian LaMachia, head of CAPI development at Microsoft was "stunned" to learn of these discoveries, by outsiders. The latest discovery by Dr van Someren is based on advanced search methods which test and report on the "entropy" of programming code.

Within the Microsoft organisation, access to Windows source code is said to be highly compartmentalized, making it easy for modifications to be inserted without the knowledge of even the respective product managers.

Researchers are divided about whether the NSA key could be intended to let US government users of Windows run classified cryptosystems on their machines or whether it is intended to open up anyone's and everyone's Windows computer to intelligence gathering techniques deployed by NSA's burgeoning corps of "information warriors".

According to Fernandez of Cryptonym, the result of having the secret key inside your Windows operating system "is that it is

tremendously easier for the NSA to load unauthorized security services on all copies of Microsoft Windows, and once these security services are loaded, they can effectively compromise your entire operating system". The NSA key is contained inside all versions of Windows from Windows 95 OSR2 onwards.

"For non-American IT managers relying on Windows NT to operate highly secure data centres, this find is worrying", he added. "The US government is currently making it as difficult as possible for "strong" crypto to be used outside of the US. That they have also installed a cryptographic back-door in the world's most abundant operating system should send a strong message to foreign IT managers".

"How is an IT manager to feel when they learn that in every copy of Windows sold, Microsoft has a 'back door' for NSA - making it orders of magnitude easier for the US government to access your computer?" he asked.

## **Can the loophole be turned round against the snoopers?**

Dr van Someren feels that the primary purpose of the NSA key inside Windows may be for legitimate US government use. But he says that there cannot be a legitimate explanation for the third key in Windows 2000 CAPI. "It looks more fishy", he said.

Fernandez believes that NSA's built-in loophole can be turned round against the snoopers. The NSA key inside CAPI can be replaced by your own key, and used to sign cryptographic security modules from overseas or unauthorised third parties, unapproved by Microsoft or the NSA. This is exactly what the US government has been trying to prevent. A demonstration "how to do it" program that replaces the NSA key can be found on Cryptonym's [website](#).

According to one leading US cryptographer, the IT world should be thankful that the subversion of Windows by NSA has come to light before the arrival of CPUs that handles encrypted instruction sets. These would make the type of discoveries made this month impossible. "Had the next-generation CPU's with encrypted instruction sets already been deployed, we would have never found out about NSAKEY."

 [send article](#)

---

### **Kommentare:**

[High Security \(Freaker, 9.1.2000 13:01\)](#)

↑ top

Copyright © 1996-2001. All Rights Reserved. Alle Rechte vorbehalten  
Verlag Heinz Heise, Hannover  
last modified: 18.07.2001

[Privacy Policy / Datenschutzhinweis](#)



editor