No. 91. Security and Your CPU

- by Stan Kaplan, WB9RQR
105 Martin Drive
Port Washington, WI 53074-9654
(262) 284-9346
skaplan@mcw.edu

CPU stands for Central Processing Unit, the "mother of all chips" on your computer's motherboard. Most of us are using Pentium CPUs at present, all of which are manufactured by the Intel Corporation. There a quite a few different models of the Pentium chip, but our story today deals with some Pentium II and all Pentium III CPUs.

Intel embedded a unique serial number in each chip during its manufacture. This number is similar to the serial number found on many devices, even the VIN number on your car. The number is hard wired inside the CPU. It cannot be altered or erased, but it can be accessed by software. According to Intel, this feature was added to help corporations track their assets, and to help consumers during online shopping and information sharing. When first implemented, this CPU ID was always on (accessible), though Intel later provided a utility program to turn it off (described below). Pressure from a number of security groups and even the American Civil Liberties Union got through to Intel, and newer models of the Pentium III have it turned off by default. It can be turned back on by software.

What does turned off or on mean? If you have a computer with a late-model Pentium III chip, when you boot that machine, the CPU ID feature is turned off by default. That means if you visit a website that can utilize the CPU ID, the site will not be able to access this unique number from your machine. If you enable (turn on) the feature, or if you have an older CPU that had the feature turned on by default, the CPU ID can be accessed over the web. Thus, we can see, there are two types of CPUs with regard to this feature. Lets call them DOFF and DON for default-off and default-on.

Which kind do you have? There is no way to tell, short of using a software program. Actually, Intel supplies a free program that makes it unimportant whether you have a DOFF or DON CPU. It is unimportant because the program allows you to set the CPU ID whichever way you want it. They call the program the Intel Processor Serial Number Control Utility. The download filename is PSENG103.EXE. Version 1.03, released 12Apr1999, is just over 1 Mb in size. You can get it from several places on the web, but I recommend downloading it direct from Intel. Go to:

http://support.intel.com/support/processors/pentiumiii/psover.htm

to get a copy. If you have any trouble getting it, send me a 1.44 Mb floppy and an SASE; I will be happy to make and send you a copy.

PSENG103.EXE is a self-extracting zipped file. Double-click it to unzip it, and then double-click the unzipped SETUP.EXE to install the program in a subdirectory of your choice and run it. When run, a blue, circular icon will appear on your system tray. If there is a white X in a red background partially covering the icon, the processor serial number is disabled. An uncovered icon indicates it is enabled. Right clicking the icon and selecting STATUS will let you see the serial number itself, if the CPU ID number is enabled. If you select SETTINGS, you can enable or disable the serial number. Note however that if the serial number is already disabled, to enable it you will have to select that option in the SETTINGS screen and follow that with a reboot. Only then will you (or a web site) be able to see the actual serial number. This nice security feature – requiring a reboot to enable the number - is actually built into the CPU itself (Nice work, Intel, you deserve a

commendation!). On the other hand, no reboot is needed to disable the number when using this program.

If you have a DON type CPU, the CPU ID feature is turned on every time you boot the computer. On the other hand, if you install the utility described above and elect to turn the CPU ID off, the software remembers the setting and will turn it off each time Windows is started, regardless of the fact that it is turned on automatically at boot time. In any case, a quick glance at the icon in the system tray will tell you immediately whether the CPU ID is on or off.

Intel may have raised many hackles when they created the unique CPU ID, but everything seems to indicate that they did it in good faith and did not intend to violate the privacy of consumers. Furthermore, they did change production so that all subsequent units that come from the factory are of the DOFF type. Finally, they provide a free utility that lets you see the status of the CPU at any time, and lets you change that status as you wish. It is hard to fault their record of accomplishment in the matter.

On the other hand, fellow hams, a hacker can obtain the CPU ID whether it is turned on or off! Easily! That is a fact! Check out:

http://www.hardwarecentral.com/hardwarecentral/tutorials/159/1

to see the two simple lines of assembly language code that will steal YOUR number and substitute that for theirs whenever software calls their machine for an ID. It really is very easy. All they have to do is download a tiny program to your machine and run it. How can they do that, you say? Well, they cannot, if you have a firewall in place. You say you did not download a free copy of the firewall Zone Alarm when I told you to? Tough. You'd better go back to No. 79 in this series, June 2000, to read about Zone Alarm. A great program, and it is free. Get it!!! Happy Computing.