Intel's Pentium III Case[i]

Objective

The objective of this report is to explore the controversy recently generated around Intel's Pentium III microprocessor by its inclusion of a unique identification number in its design. The ID number can be configured to be visible or invisible to the operating system with the use of software. The unique identification of a specific computer carrying such a processor has generated praise for its security implications but scorn for its privacy consequences. In this report, we will consider both sides of the debate and conclude with a discussion on whether the chip should be shipped with the ID number visible as the default or not.

Background

The increasing use of the Internet for communications and electronic commerce is raising PC users' concerns about the confidentiality and integrity of transaction-oriented data. Since computers are the primary connections to the Internet, they are a logical place to add security features[i]. The vision of millions of interconnected trusted computers cannot be realized unless encryption mechanisms are designed to provide security for authentication. The computer is a good place to start as it is a physical node on the network (software is a virtual one). Intel is a

[i] Intel, Pentium III are registered trademarks of Intel Corporation.

leader in this domain, although it is not alone in this effort as other processor manufacturers are contemplating adding features that improve security.[ii]

In late January this year, Intel Corporation announced that it planned to launch its new Pentium III processor that would include a processor serial number (PSN). The Pentium III processor was designed with the Internet in mind. One of its new features is an embedded electronic identification number built in to the core of every Pentium III processor. Known as the processor serial number or PSN, this feature is supposed to benefit consumers by providing an increased level of security on the web. For example, the PSN, in combination with user name and password, can strengthen the security for e-commerce, members-only chat rooms and many other web-sites with restricted access by identifying the processor and the PC when a user connects with another site or system

The identification process relies on a software utility that will be installed by PC manufacturers or maybe built into future operating systems. This software will interface with the processor and the browser. When a Web site asks the browser to authenticate an ID, the browser calls the utility software that interrogates the processor and returns an ID number. The browser, then, transmits the ID number to the Web site.

The Controversy

Soon after Intel's announcement, different privacy groups started a campaign against the measure, arguing that this identification system violates the privacy of Internet users by allowing third parties to identify and collect data on Web surfers. Junkbusters, Electronic Privacy Information Center, and the Center for Democracy and Technology led the coalition of privacy groups attacking Intel over the new PIII feature. The coalition's boycott hit the company hard and included letters to US Congressmen, the FTC, and Mutual Funds holding Intel stocks and the media in general.

After some days of consideration, Intel finally decided to ship the processor with the PSN in the "off" position in order to soften the adverse publicity generated by this situation. The company also said it would offer software that would allow users to switch the PSN on and off and alert them if the PSN's mode was to be changed. Despite these steps, privacy groups did not stop there, and decided to expand their call for a boycott to include any PC manufacturer that ships a Pentium III system with the ID number, not just Intel.

Intel argues that the Pentium III processor owner will be able to make choices about how to use the processor serial number. According to Intel, the processor serial number does not and cannot transmit or "broadcast" information over the Internet. In general, a user will need to explicitly allow the reading of processor serial number by a web-site. In order to read the processor serial number, a web-site will need to run a program on the user's system. The default security setting of popular web browsers alerts a user before permitting a program to be executed. In keeping with "safe web surfing," users should exercise caution before allowing any program to be executed from an unfamiliar web-site. Users concerned about a particular web-site's use of their processor serial number may refuse to download and/or run the program.

On the other hand, people fear that the PSN might allow Intel to spy on people, to act as some type of Trojan horse that would collect information about the user and report back to Intel. However, Intel claims that this Processor Serial Number is just a number, a piece of information on the chip, and it does not have the capability to send or receive information. Intel also has a Privacy Policy statement, which states that no personal information tracking will take place within Intel utilizing PSNs. Despite Intel's explanation, there is a fear that Internet companies and commercial institutions, as well as software companies that want to fight piracy will push the PSN as a standard and prerequisite in web surfing and e-commerce.

In any case, controversy has intensified and the issue is not yet fully resolved. On the one hand, advocates of Intel's chip argue that the PSN is not accessible, if it is in the "off" position. On the other hand, privacy groups have warned that it is not in Intel's control to put the switch "on" or "off" but in the computer manufacturer's control. Moreover, they have argued that the software provided by Intel is easily "hack-able" so even if the PSN number is turned "off", hackers would have the ability to enter a remote system, change the status of the PSN and from there, start misusing the PSN information. In the following section of this paper we will analyze in detail the pros and cons of the referred chip, what should be done to preserve privacy on the internet, and what are the potential consequences of having such a chip in the market.

What is PSN?

Before dwelling in the realm of the controversy, perhaps it would be appropriate to provide a more technical explanation of how this new feature works. The Intel processor serial number (PSN) feature is embedded into the chip during the manufacturing process of the Pentium III processor. A unique PSN for each processor can function as an authentication feature in e-commerce, remote management of corporate PC's in a network, enhancing security on the internet, and acting as a username and password for web-sites.

The Processor Serial Number starts out as a 96-bit number, a string of 96 zeros and ones, on the processor. This is put on during manufacturing as a physical part of the processor. It can not be erased or modified by the user. While it is 96-bits, the actual PSN is the last 64 bits, this is a different number for each processor. The first 32-bits is the CPUID, which has been in place since the later i386 processors and contains encoded information about your specific processor that can be read by certain pieces of software.

The CPUID identifies the following:

(1) whether the chip is actually an Intel chip (identified by the ASCII string "GenuineIntel")
(2) its processor type (whether it's single or dual) and family (i386, i486, Pentium, MMX, etc),
(3) the model number (used in conjunction with the family to more precisely identify the processor)
(4) the stepping (used to track revisions made to the processor since "A" stepping, when it first comes out)
(5) and for later processors such as the Pentium Pro and the Pentium 2, the cache information

The 96-bit PSN is used by two new instructions on the Pentium III processor. The first instruction is the read instruction, which when executed by a program, the 96-bit PSN is returned to that application. The second instruction, the disable instruction, is the one that people are so interested in; it manipulates the Model Specific Register bit. When that bit is set to 0, the last 64 bits of the PSN is unlocked and the first instruction can return the processor specific PSN. When the bit is set to 1, the last 64 bits of the PSN is locked and can not be read but the read instruction can still return the CPUID.[iii]

Initially Intel had planned the Model Specific Register is 0, or on by default. Intel’s Processor Serial Number Control Utility, then, can be installed to control the reading of the PSN; Intel has asked PC vendors to install this extension into the software. This works in Windows (a version is being developed for Linux systems) to determine the state of the Model Specific Register bit, set the state to 0 or 1, and to read the value of the PSN. A user can have this utility set the register the state to off whenever Windows boots up. However, while the PC is on and before Windows loads the application, the state is on, so to combat this, the register can also be modified in the system BIOS. Intel is helping motherboard manufacturers create BIOS software that supports the manipulation of the register bit; by doing this, a user can have the PSN turned off when the computer turns on. To further aid the user, the register can be turned off without rebooting the system, but has to be rebooted when turning it on. This is a layer of security in preventing web-sites from turning on a register that is set to be off at boot-up and reading the PSN without the user knowing. Due to raised campaign against this feature, Intel is shipping the new processors with the PSN off as default.

The Pros

The controversy has been over the benefits and the costs of this implementation. In this section we explore the pros of using a unique global identifier on your computer and why the processor is a good place to put it.

Stronger security

The biggest advantage of enabling the PSN feature is security. Higher security benefits e-commerce, government, and in turn, consumers. The benefits of having higher security implemented can be observed in the following IT areas: secure transactions, tracing wrongdoers, intellectual property management, and preventing over-clocking.

Secure transactions

On-line fraud is a rising concern for the e-commerce community. On-line fraud takes place as an elevated form of credit card fraud, and at any case its victims are merchants, not customers. Bill Headapohl, President and Chief Operating Officer of popular online software retailer BuyDirect.com recalls, "our fraud rate was over 20%." For the most part, traditional methods of credit card verification proved inadequate. "If someone uses a card that doesn't belong to them, and Visa says it's good, but the true cardholder later denies the charge, the merchant can never win," Headapohl explains[iv]. Internet fraud detection and solution company cybersource.com currently provides services on real-time deliverable addresses for e-commerce companies. Adding the PSN to security procedure can possibly reduce the risk of fraud.

E-commerce web-sites can crack down the on-line fraud by demanding a PSN be sent in encrypted form, enforcing a no number-no sale practice. Used in combination with other ID attributes such as credit card number and login, the PSN prevents fraudulent transactions. Also, software utilizing the PSN can monitor whether an outside user is trying to hack into the corporate network. The on-line activities can be business-to-business or business-to-consumer transactions. The idea is to provide maximum trust equivalent to the face-to-face transaction for electronic transactions.

Tracing Wrong-doers

Cyber crimes have become a major problem that affects the e-commerce community, the government and, consumers as a whole. And the problem is expected to only grow as the use or the function of the Internet expands day after day. The cyber crime includes hacking into corporate databases and individuals’ computers, spreading fraudulent announcements, spreading viruses, and many more. In many of the crimes, any sort of tracing method or evidence would provide information for law enforcement agencies.

For example, the recent arrest of email virus Melissa's creator David Smith was possible only with the help of a unique number that came from Word 97 processor and fingering through AOL connection. The law enforcement uses other electronic fingerprints known as Global Unique Identifier (GUID) and IP address of an email through the ISP. The IP address only identifies the physical location of ISP, not necessarily the location of the user.

Internet stock-fraud schemes are also proliferating as about 7.5 million Americans buy and sell stocks over the Internet and that number is expected to grow to 18 million by 2002. The schemes can arrange from selling the stocks of a non-existent company, announcing false messages and fraudulent transactions. The Securities and Exchange Commission reports that it receives about 200 to 300 electronic-mail complaints daily about potential Internet fraud, up from 10 to 15 daily complaints in 1997. Since 1995 the agency has opened 66 investigations into Internet stock fraud cases and has concluded 32 of them[v]. Adding a PSN, as another layer of security, can initiate a mechanism of disclosing the location and the identity of fake announcement or fraudulent transactions, therefore, reducing the Internet stock scams.

Intellectual Property Management

Intel claims that the new PSN utility will make software piracy more difficult. Software vendors have been fighting unauthorized software distribution to protect their copyright as well as their software revenues. The PSN feature can function as a tool to verify their software licenses. One would register his copy of a particular software which remembers the PSN upon installation. The stored PSN in the software will then prevent subsequent installations from the same disk or CD-ROM. In this way, software companies can reduce the sharing of software and are able to impose lower prices, as they do not have to adjust pricing for losses from illegal copying.

The feature has far-reaching implications for protecting online copyrighted material. The serial number would create an electronic stamp of the material's point of origin, For software manufacturers, the new chip feature shows promise as a weapon against piracy. If each software license can only be used on the computer with the correct serial number, the market for pirated software goods essentially evaporates.

Preventing over-clocking

The use of the ID scheme can also solve illegal over-clocking problems that have plagued Intel for some years. Over-clocking is an act of running a processor at a higher speed than that specified by its manufacturer. Hardware hackers can easily achieve the over-clocking by assembling a high-speed bus with the processor. Intel has encountered the over-clocking problem because computer companies are able to buy a 300 MHz Celeron processor, over-clock it to 400 MHz and sell it as a 400 MHz-processor to consumers.

The over-clocking problem addresses two issues for Intel. First, it results in profit loss for Intel since the computer vendors or even hacker-individuals can take advantage of obtaining high-speed processing power at a lower price. More serious problem of over-clocking is a reliability issue. Given the proper cooling and technique, over-clocking will enhance the performance of a computer through faster processing, however, the computer system may be damaged without the proper handling. The reliability issue also applies to a situation where a processor does not reach the vendor-specified-over-clock speed. This will damage Intel's reputation, not the PC vendor.

With the electronic ID number embedded in each processor, the consumers will be able to check their processor against Intel's database of products to find out the original clock speed of the processor specified by the manufacturer, hence, they are able to identify fraudulent PC-makers. This still leaves freedom for the PC hobbyists who want to over-clock their processor privately at their homes[vi] and at their own risk.

PC asset management

Computer is becoming an increasing part of corporate assets. Corporate and education institutions with large computer assets usually assign a serial number or a label on each computer for future tracking and better management. The PSN can be used for information management and PC assets management by Information Technology departments. This is in a sense a more practical way of keeping track of the physical computer infrastructure of a corporation.

Privacy

If privacy is a concern, one shouldn't use the Internet since the Internet connection itself already discloses a lot of information about the user through IP address and cookies. There are more identifiable fingerprints upon the use of the Internet that intrude the privacy of the user; however, they are not as much of an argument for privacy advocates. Bill Machone said: "Do you have an Ethernet card in your system? If so, it already has a unique ID, Now two NICs on the planet have the same MAC address. It's been there forever. Do you hear stories about NIC abuse and constitutional freedoms?"[vii]

Summary of Pros

The PSN itself will not halt the cyber crimes and fraud, however, in combination with other ID features and infrastructure, it is highly potential that the Internet security will improve. This requires cooperation between hardware and software communities, consumers, government and law enforcement agencies. Having an extra layer of traceable element seems to promise improved security.

The privacy advocate might be exaggerating the issue over the PSN feature as disclosing most personal information over the Internet. In reality, however, we all give out our social security numbers to credit card institutions, bank, landlords and other groups of people. In many times, the disclosure is not required, but provided out of free will. Drawing a line of privacy on the PSN feature, therefore, seems random at most.

If the computer industry can create trusted, secure systems, then there should be no need for to intervene in the market with regulation of encryption, intellectual property restrictions. The PSN is the beginning of an effort towards the much-coveted "self regulation" policy.

The Cons

In this section we provide the arguments against the used use of the PSN. The main opposition comes from the privacy groups. Arguments are also provided against the points discussed in the pros section of this report.

Privacy

The fact that the PSN can be remotely read by web sites and other programs in mass-market computers would significantly damage consumer privacy in the sense that the number could be used to link user's activities on the Internet for marketing and other purposes.

The PSN would likely be collected by many sites, indexed and accumulated in databases. Unlike cookies, which are usually different for each web site, the PSN will remain the same and cannot be deleted or easily changed. The advertising and marketing industries have been strongly advancing technical means of synchronizing cookies so that information about individual consumer behavior in cyberspace can be shared between companies. The records of many different companies could be merged without the user's knowledge or consent to provide an intrusive profile of activity on the computer. The only solution would be to change the processor or computer. Because the US has few legal protections for online privacy, there are no practical limits on what can be collected or used.

Internet Security? Where?

According to Internet security experts, the PSN will not provide real security because it is poorly designed. Hackers will be able to forge PSNs, thus undercutting potential authentication uses. Noted cryptographer Bruce Schneier, author of *Applied Cryptography*, recently wrote the following:

> "The software that queries the processor is not trusted. If a remote Web site queries a processor ID, it has no way of knowing whether the number it gets back is a real ID or a forged ID. Likewise, if a piece of software queries its processor's ID, it has no way of knowing whether the number it gets back is the real ID or whether a patch in the operating system trapped the call and responded with a fake ID. Because Intel didn't bother creating a secure way to query the ID, it will be easy to break the security."

Moreover, some companies have already announced they have hacked the system. This is the case of Andreas Stiller, processor expert of c't magazine, a German technology magazine, who has write a program which accessed the serial code embedded in the chip without alerting the user, despite Intel's assurances that the code can only be read with a user's agreement. This procedure is based on specific features of the system architecture that are documented.

The conclusion is obvious. The threat of being hacked is real and Intel has confirmed that any online system is a potential target for hackers looking for the referred PSN. Once hackers get the processor serial number, they could potentially impersonate the real owner of the computer, and participate in transactions and operations that would have disastrous consequences. Is the PSN worth the risk? Clearly not.

Inconvenience

Beyond the privacy issue, the PSN can become an inconvenience for people who use more than one PC or for several people who share one computer. This is very common, and that simply defies the idea of having an identity linked to a single PC. Other problems can arise from upgrading systems, which can cause additional inconvenience to the user.

Using the PSN to prevent chip theft and over-clocking

Chip theft is an important issue and thefts cost the industry and Intel millions of dollars each year. However, Intel has stated that the PSN is not designed to be used for either preventing chip theft or limiting over-clocking. In fact, the company has declared that does not plan to keep track of the PSN.

The PSN versus other identifiers

The Intel PSN is a unique identifier that will be placed in nearly every consumer's computer. Intel currently dominates the microprocessor market with over 75 percent of the market. Intel has stated that it plans for the PSN to be widely adopted for electronic commerce and authentication purposes on the Internet. Because of the possible wide adoption and Intel's plans for broad uses for the PSN, it raises privacy concerns may not arise with other identifiers.

Some expensive business computers, such as workstations sold by Sun Microsystems, do include a form of a PSN but they are not widely used by consumers. This small market share has prevented the adoption of their PSN as an identifier, except for limited software registration.

Internet Protocol (IP) addresses are not as permanent as the PSN. When users of the Internet visit a web page, their IP address may be revealed to the web page machine. Many users do not have a permanent (static) IP address that can be used to trace their movements. Users of America Online and many corporate networks use proxy servers which mask the identity of the users. Most Internet Service Providers (ISPs) provide a different IP number for each user session. Users can also change their IP addresses by asking their system administrators or changing ISPs. In addition, there are web-based services such as The Anonymizer that prevent the disclosure of their IP address.

Ethernet IDs are not widely available and are not intended for identification. Ethernet identities are used for routing computers connected to networks via Ethernet and are not collected or used for identification purposes. Currently, most users connect to the Internet via modems and serial ports so Ethernet IDs are not used or disclosed. Many computers simply do not include Ethernet cards. For those that do, users can also buy inexpensive new Ethernet cards without changing the processor or buying a new computer.

Other identifiers are not widespread. Other identifiers available include other hardware items, and software registration codes. But none of the hardware items are likely to be available on a majority of consumers' computers, and browser manufacturers are unlikely to transmit license numbers with every web page request, so these are not likely candidates to become the "social security number" of a PC. The PSN was designed to be widely used as an identifier.

A Disabled PSN is not enough

As commented in the introduction of this paper, Intel announced that they were planning to release a software program that would turn the PSN function "off". This program will run automatically each time a computer is booted and turn the PSN off for that session. However, the PSN function will remain in the Pentium III chip and will be available if the program is disabled for any reason. Some of the problems are as follows:

- This program does not exist yet. According to the *Washington Post*, the program will not become available until months after the first PIII-enabled machines are shipped and even then will only work for Windows users. Users will be required to access the Intel web page to obtain a copy of the program and install it themselves.

- This approach relies on other companies to install the program for Intel. When the program does become available, Intel will have to ask every computer manufacturer and other computer companies, including Microsoft, to adopt this into their systems. Some of these companies, such as Microsoft, which have an interest in using the PSN for software verification, may refuse to install the program.

- Users will be required to provide the PSN. It is likely that users will be required to disable the PSN privacy protections by many software programs and web sites as a condition for access. According to Intel VP Patrick Gelsinger, many software developers are already planning to use the PSN and would be likely to require that the patch be removed: "We're very happy and actually rather surprised by the amount of enthusiasm we've gotten from application developers for the processor serial number capability. We have some 30-plus applications today that have committed to take advantage of this. And that number is rising very rapidly." For web-based applications, many web sites already prohibit access if the user will not accept cookies. If the PSN becomes an industry standard, users will be required to provide their PSN as a condition for access. Gelsinger has already suggested that it be used for chat rooms "where unless you're able to deliver the processor serial number, you're not able to enter that protected chat room."

- The software program can be tampered with or disabled. Because the privacy protection scheme relies on a software patch that must run each and every time that a user turns on the computer, it is susceptible to tampering by other software programs. Programs such as word processors or web browsers which must be installed onto systems could easily disable the patch in the installation process. Web-based Java applets could also be used for this purpose. A hardware solution is the only permanent option to this problem.

Unknown Implications

The major risks of the technology, however, rely in the fact that potential forms of misuse would be difficult to detect until it is too late. As Deirdre Mulligan - staff council at the Center for Democracy and Technology - commented, "The hard part is figuring out implications. Until it's put out into the marketplace, it is difficult to tell", she added. "Like law, software code has great social implications for privacy and speech.".

Summary

The PSN does compromise privacy as admitted by Intel officials (reference?). At the same time, it is questionable that the PSN will result in major improvements of security. The improved security seems to affect more the average user (at the expense of their privacy), but it is obvious that malicious users will still have plenty of room to continue their activities unaffected.

The privacy advocates seem to be serious about boycotting Intel's chip if they don't backup. And there's a valid reason for that. At a time when the future of the web is being determined, the PSN would set a bad precedent.

We have also included a set of links to articles on the topic in our group's web site.

[i] http://support.intel.com/support/processors/pentiumiii/psqa.htm
[ii] http://www.zdnet.com/filters/printerfriendly/0,6061,2192323-2,00.html
[iii] http://www.thebee.com/bweb/iinfo141.htm

[iv] http://www.ecommercetimes.com/news/articles/981204-1a.shtml
[v] http://www.computernewsdaily.com
[vi] http://www.zdnet.com//filters/printerfriendly/0.6061,2189721-2,00.html
[vii] http://www.zdnet.com/pcweek/stories/printme/0,4235,388214,00.html