Cyber-Rights & Cyber-Liberties (UK)

Report on the Intel[1] Pentium[1] III Processor Serial Number Feature

Introduction

Recently Intel have announced that the new Pentium III processor, due for release in the first quarter of 1999, will contain a feature known as a Processor Serial Number (PSN). Each processor will have a unique PSN combined with two machine instructions, one that allows software to read its value and another that disables any further access to it. After access to the PSN has been disabled, the read instruction no longer returns the value and access is only re-enabled when the processor is reset, for example, by restarting the machine.

Control of Access to the PSN

Intel is proposing that access to the PSN on Pentium III based PCs should be controlled in either of two alternative ways:

- The first method of control is provided by a software control utility that is loaded and run when the Windows[1] operating system is started (when a machine is switched on or rebooted). Intel is recommending that this utility defaults so that PSN access is *disabled*.
- The second uses control in the PC's BIOS where a CMOS configuration setting will be used to enable or disable PSN access according to the owner's wishes. Where this is provided Intel is recommending that the default setting should *enable* PSN access.

Consequences of the Intel Recommendations

If Intel's recommendations are followed, when a Pentium III based PC is first switched on PSN access will be enabled by the default setting in the BIOS. Access will then be disabled later when the control utility is run during the start up of the Windows operating system. Between these events PSN access is enabled and this means that the Windows operating system can access the PSN irrespective of the owner's wishes as expressed through the setting of the software control utility.

Moreover, since any installed software can request that Windows runs one of its components during Windows start up, any installed software can also read the PSN before it is disabled by the control utility (a PC reset has to occur after installation but this will be the norm for installed software). As a result any software that a PC owner installs on their PC can also read the PSN irrespective of their wishes as expressed through the software control utility.

For owners who want stronger control over the PSN feature Intel is recommending that this is available through a BIOS configuration option. Intel's current recommendations to

[1] 'Intel' and 'Pentium' are recognised as trademarks of Intel Corporation. 'Windows' is recognised as a trademark of Microsoft Corporation.

PC manufacturers suggest that this level of control should be provided and a number of recommendations are made to ensure that it remains effective during PC use.

However, it is unlikely that most PC owners will be able to set their PC's configuration settings. This will be either because manufacturers have not provided this BIOS configuration option (although recommended, it is optional), or because they are not sufficiently skilled or confident to alter the CMOS setting.

As a result, Intel's recommendation that the BIOS should default to allow PSN access will mean that installed software applications on most PCs can technically obtain the value of the PSN irrespective of the wishes of the owner. We will consider later whether it would be lawful to access the PSN against a PC owner's wishes.

Potential Benefits of a Processor Serial Number

Additional Consumer Security

A PSN may allow owners to benefit from an extra layer of authentication to protect themselves from fraud. For example, in an electronic transaction in addition to a name and password they will also be able to specify that their financial transactions can only be authorised on a PC having their own PSN. If implemented properly this could add to the safety with which such transactions can be pursued.

At the moment, however, the added security that this approach can offer is limited by the security of the software that performs PSN checking on an owner's PC. In practice, fully secure software is not feasible and most PCs are not very secure either. In consequence it is hard to see that a PSN will offer large gains in security until these weaknesses are overcome.

Corporate PC Asset Management

In a corporate environment with many PCs, the PSN feature will make PC asset management easier.

Corporate Information Management

A PSN may also assist in advanced information management tasks where it is appropriate to ensure that critical corporate information is closely controlled.

Combating Chip Theft and Fraud

A PSN could be of considerable value in tracking stolen processor chips and hence combating chip theft. It could also be used to prevent fraudulent traders from selling PCs with over-clocked processors in place of the genuine, properly rated products. However, it appears that Intel is not pursuing these possible uses of the PSN.

Potential Risks of a Processor Serial Number

Privacy - Removing or Weakening Pseudonyms

Some people wish to hide their identity in cyberspace by operating under pseudonyms. It is likely that such people will often operate from the same PC, where the availability of a means to read its serial number might enable a remote agent to discover a link between different pseudonyms and hence discover information about a person's identity that the individual wishes to keep private.

Beneficial uses of pseudonyms could be undermined. For example, in some countries they facilitate political free speech without fear of persecution. Anonymity and

pseudonymity allow people in countries where human rights and democratic freedoms are not respected to express their views with less fear of persecution.

Of course, pseudonyms also bring risks for society as well as benefits and this makes it important to achieve a careful balance between these opposing pressures in deciding how a PSN feature should be controlled.

This is one of a number of ways that a PSN might be used to reduce a user's privacy. The large-scale collection and correlation of identity and PSN data might be another example of abuse.

It is hence possible that the easy availability of a PSN could lead to a number of privacy abuses.

Software or Content Tied to Particular PCs

The availability of a processor serial number may allow software and information (content) suppliers to configure their products in such a way that they will only work on specific machines. Some content is 'use once only' and this does not seem problematic but most software and most content may need to operate on more than one PC. This would be the case, for example, where a PC is replaced with a new one, with the owner's software being moved onto the new machine. In such circumstances a lawful software owner could find that their software suddenly becomes inoperative in the absence of a tedious and very lengthy process of re-registration with a new PSN.

On the positive side of this equation a PSN may prove useful in reducing the level of software theft and this could have benefits for consumers who would no longer bear the overhead costs of illegal use. In theory a PSN could have uses in combating software and Intellectual property theft and its easy availability might spur such developments.

In practice, however, experience with software protection schemes shows that these often work to the disadvantage of lawful owners through the considerable inconvenience that they can cause. For these reasons, it is not self evident that a PSN will work to the advantage of lawful software and content users.

At present, therefore, the value of a PSN in combating the illegal use of software and content is unclear. Until the uses of PSN's for such purposes are better understood, it is reasonable for lawful users to see this as a possible area of risk where their interests could easily be undermined by ill thought out schemes.

Processor Serial Number Access - Vulnerabilities

As already discussed in outline, the vulnerability of the PSN to being read against a PC owner's wishes arises from software that the PC owner installs (or allows to be installed) on their PC.

The recommended software control utility gives a measure of control over access that should deter ethical software suppliers from reading the PSN but the nature of modern PCs is such that this can be bypassed technically by any determined software supplier. Although this requires that the PC be restarted, this is a common event during software installation, which means that access to the PSN is not difficult to achieve in such circumstances. Moreover, this can be done covertly without the PC owner's knowledge and consent should a software supplier choose to do this.

For owners who want stronger control, Intel has recommended that PC manufacturers should provide BIOS level control of PSN access. This form of control will be significantly stronger than that provided by the software control utility. It will not be

technically impossible to bypass it but those doing so will have to work harder to achieve this. If BIOS access control is implemented well, software suppliers will have to interfere with the PC's BIOS or its CMOS configuration data to do this. At very least such action could only be seen as highly irresponsible; at worst it would be a criminal act since it could easily damage a PC and cause it to fail completely.

In the UK, the Computer Misuse Act 1990 is almost certain to make the reading of the PSN against an owner's wishes illegal. Section one of this Act states:

- A person is guilty of an offence if:
  - he causes any computer to perform any function with intent to secure access to any program or data held in a computer;
  - the access he intends to secure is unauthorised; and
  - he knows at the time that he causes the function that that is the case.

It seems certain that this will apply whichever form of control a PC owner chooses (BIOS or software utility) but unauthorised attempts to read the PSN by making BIOS changes would probably be treated as especially serious in view of the damage such actions might cause.

It is also possible that the European Union Data Protection Directive could make it illegal to use the PSN feature in any way that undermines privacy or personal data protection.

In practice attempts to read the PSN against a PC owners wishes are only likely to be pursued by highly unscrupulous suppliers, by hackers and, possibly, by law enforcement and Intelligence agencies where they see access to a PSN as vital to their specific interests. Unfortunately, these are precisely the organisations that are unlikely to respect legal safeguards and those that will often be exempted from their provisions.

The possibility of the PSN to being read by installed software against a PC owner's wishes is hence a technical one for which there are legal safeguards in the UK (and probably many other countries as well).

The technical possibilities for access can hence be summarised as follows:

PSN access control approach	**likely to deter**	**Unlikely to deter**
Software control utility	ethical software suppliers	Unethical software suppliers; Hackers with malign intent; Virus and worm writers; Law enforcement agencies; Intelligence agencies.
BIOS level access control	all software suppliers	Hackers with malign intent; Virus and worm writers; Law enforcement agencies; Intelligence agencies.

Owners need to decide for themselves whether these possibilities might create wider risks for them within the context in which they use their PCs.

Discussion

In view of the reaction to Intel's PSN announcement, there can be little doubt that this feature is controversial. A consequence of this has been an emotional and heated debate about the true benefits and the potential risks that this feature will bring. It seems rather unlikely, however, that this debate will lead to any consensus on these matters and this means that only time will tell which arguments prove to be correct.

However, in the opinion of Cyber-Rights & Cyber-Liberties (UK) ("CR&CL(UK)") much of this debate misses the point because it is not the benefits or the risks as such that really matter but rather the issue of who is able to make the decision to take these benefits while accepting the risks that are also involved.

CR&CL(UK) is firmly committed to the view that PC owners and cyberspace consumers should never be exposed to any risks without their explicit consent, irrespective of the benefits that this might bring. Such decisions belong to PC owners and are their's alone, and no-one else has the right to make such decisions on their behalf without their involvement.

It is wrong in principle for any party to pursue actions that undermine the ability of PC owners to make their own trade-offs between benefits and risks in areas which impact on their security, safety or privacy. By introducing the PSN feature with inadequate prior consultation and public debate, Intel has sought to make this decision on behalf of PC owners and has, in consequence, deprived them of the right to do this for themselves. We accept that this may well have been unintentional but it has happened nevertheless.

CR&CL(UK) does not have any doubts about Intel's desire to improve security for its customers. We are, however, surprised to be faced with a 'fait accompli' on such an important issue. We are also surprised to be put in this position by a company that has a global influence on the safety, the security and the privacy of millions of consumers. We simply cannot accept that such steps should be taken without the widest possible public consultation.

CR&CL(UK) does not object on principle to the introduction of a PSN. But we do object, in the strongest terms, to the way this has been done. If Intel wishes to maintain the trust and confidence of its customers, it must conduct adequate and timely public consultation on those features that it intends to introduce that might directly affect their safety, security or privacy. And it must do this in a way that allows those who have genuine concerns to achieve some influence over the course of events.

CR&CL(UK) recognises that the extreme pressures of market competition faced by Intel impose a strong desire for secrecy in the development and introduction of new products. Unfortunately, however, such pressures work directly against the requirements for open debate and public review that are essential if real improvements in cyberspace security and privacy are to be achieved. Ultimately, therefore, Intel (and its major competitors) will have to make difficult policy decisions about their work on product features designed to improve security and safety for their customers – they will need to decide whether short term market advantage is more or less important to them than fostering the long term trust and confidence of their customers.

CR&CL(UK) believes that it would be irresponsible for any company to put the safety and security of their global customers at risk in order to gain short-term market

advantage. Moreover, we believe that such actions would never be in the true interests of the company concerned.

> **We therefore call on Intel and other major processor suppliers to co-operate rather than compete in the introduction of those specific features in their products that are intended to provide improved safety and security for users of the global information infrastructure (cyberspace).**
>
> **We also call on these companies to pursue such work with effective and timely public consultation and in a manner that allows their global customers to have an influence over the course of events.**

The Way Forward

We have considerable sympathy with those who are calling for a boycott of Intel products; we understand their frustration and their anger at the way the PSN has been introduced. Nevertheless, CR&CL(UK) wishes to have further dialogue with Intel to see if there is another way forward. We earnestly hope that Intel will react positively to our proposals and, for our part, we remain ready to consider any suggestions that Intel themselves may wish to make on how such problems should be tackled in future.

CR&CL(UK) hence reserves its position and intends to review the situation and make further recommendations in the light of the Intel response to the concerns and proposals set out here.

The following paragraphs set out recommendations and requests for those involved in the supply of Pentium III based PCs or the software and services that these will support.

Intel

CR&CL(UK) recommends and requests that Intel pursue the following specific actions:

- work with PC manufacturers and suppliers to ensure, as far as is practically possible, that access to the Pentium III PSN is definitively under the control of PC owners;
- ensure that future processors with a PSN are designed in a way that allows PC manufacturers and suppliers to give PC owners full control over access to this feature;
- seek an arrangement with other major processor suppliers for co-operation on those features of products that provide for (or have a direct impact on) the safety, the security or the privacy of their customers in their use of the global information infrastructure.
- work to achieve effective and timely public consultation on such developments in a way that allows for influence over their form and their evolution

PC Manufacturers, Suppliers and Retailers

CR&CL(UK) recommends and requests that PC manufacturers, suppliers and retailers pursue the following actions:

- ensure, as far as is practically possible, that access to the Pentium III PSN is definitively under the control of PC owners;
- in order not to expose consumers and home PC owners to as yet undetermined risks, ensure that PCs are supplied with BIOS control of the PSN feature and with it in an initially disabled state;

- ensure that prospective PC owners, especially consumers and home PC users, are fully informed about the PSN and its benefits and risks.

Software (and Web/Internet Service) Suppliers

CR&CL(UK) recommends and requests that all software (and Web/Internet service) suppliers, especially major ones, make a public commitment to use the Pentium III PSN feature in an ethical way that fully respects the wishes of PC owners. We specifically request commitments:

- not to seek access to the PSN where a PC owner has disabled the feature either through the software control utility or through a BIOS configuration setting;
- to specifically request permission to access the PSN even when it is enabled;
- provide information prior to software purchase if their product makes use of the PSN feature;
- fully and precisely describe all uses to which the PSN is put;
- if the PSN is used, to do this in such a way that its value is not revealed outside their application;
- to request permission if the PSN value is to be sent from the owners PC to other locations and to provide full details of all the remote uses of the PSN.

PC Owners (Especially Consumers and Home Users)

CR&CL(UK) recommends that consumers and home PC users should:

- consciously consider the benefits and risks of the PSN feature before buying a Pentium III based PC;
- consider adopting a cautious approach when buying a Pentium III based PC by choosing one that provides BIOS level control with the PSN initially disabled.

Acknowledgements

This Cyber-Rights & Cyber-Liberties (UK) report was written by Dr Brian Gladman, Technology Policy Advisor for Cyber-Rights & Cyber-Liberties (UK). Dr Gladman has co-ordinated the CR&CL(UK) strategy in considering the privacy and security issues posed by the PSN feature following a meeting held between CR&CL(UK) and Intel representatives in early February 1999.

CR&CL(UK) wishes to acknowledge the extensive and helpful assistance provided by Intel in the preparation of this report. Particular thanks are due to Bernhard Ries and Hans-Juergen Werner of Intel for their patience in answering the many difficult questions that arose during its preparation.

Intel or its employees are in no way responsible for any of the views or opinions expressed in this report.