Could New Chip Privacy and Security Measures Tie Users' Hands?

A New Report By Cyber-Rights & Cyber-Liberties (UK), June 1999

In February 1999, Cyber-Rights & Cyber-Liberties (UK) published its Report on the Intel® Pentium® III Processor Serial Number Feature:

http://www.cyber-rights.org/reports/intel-rep.htm

We criticised Intel for failing to ensure that the serial number feature of its new Pentium® III chip would be fully under the control of the user. We called 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 cyberspace. We also called on those companies to pursue such work with effective and timely public consultation and in a manner that allowed their global customers to have an influence over the course of events.

Intel is now working actively with PC manufacturers to ensure as far as possible that the serial number feature of the Pentium® III is under the user's control.

This new report reviews some possible features of future chips, and calls for effective advance consultation about their implications.

Published research has explored the possibility of building into microprocessor chips the ability to carry out cryptographic processes. (See *The TrustNo 1 Crypto-processor Concept* by Markus Kuhn, http://www.cl.cam.ac.uk/~mgk25/trustno1.pdf, and papers there cited.) One possible application for techniques of this kind would be to build chips that would refuse to run any code not digitally signed with a cryptographic key recognised by the chip. Another possible application would be to build chips capable of running code which had been encrypted.

Such features could provide powerful protection from a number of risks. They could provide valuable protection from many kinds of viruses. They could also be used within a corporate environment to ensure that users were not running software not approved by the business. And if new software standards and certification procedures are developed for software that respects users' rights to anonymity and to the control of their own private information, such chip features could help users avoid running non-compliant software.

But such features raise two equally important questions: who is to control them? And how can users be sure they are reliable?

Control

If the manufacturer alone determines whose signature can validate a program to run on the chip, the owner of a PC is denied the right to manage their own system and decide what programs will be able to run. This is fundamentally unacceptable.

Owners may wish to write their own programs. Owners may wish to run programs provided by third parties who have not entered into arrangements with the chip manufacturer for the recognition of their signatures. Chip manufacturers may be pressed by their governments to favour some software and disfavour other. The owner would be at the mercy of unknown factors, operating without transparency or accountability, and pursuing interests which may be far from their own.

One possible example out of many is provided by Netscape's Internet browser software. As a result of US Government controls on the export of cryptographic software, this browser is exported in crippled form. If it is used to connect to an Internet web site using cryptographic protection (typically the SSL protocol), it is

generally limited to the use of 40 bit keys, which are too weak to provide any significant security. But a program is available on the Internet called "Fortify" which can be used to restore the cryptographic functions of the Netscape browser so that it uses full 128 bit keys for its SSL connections, giving strong cryptographic security.

But if the user's chip will run only the crippled version of the browser, because the full strength version has not been signed with a key recognised by the chip, then users are denied the ability to obtain the security they want. No doubt the US Government would be only too pleased if chip manufacturers could be persuaded to support its export control regime in this way.

A similar result would follow if the browser was supplied in encrypted form: it would then be impossible for an external program like Fortify to modify it so as to provide its full cryptographic strength.

This also illustrates another drawback of the use of encrypted code: the user has no way of knowing what functions are provided by the code their computer is running. At present a user can in principle get advice from experts who can examine code and say what functions it performs. This openness to scrutiny serves to ensure that users stay in control, and the use of encrypted code would undermine that control.

Reliability

The technical and procedural methods required to implement the features described in this note are complex and difficult. Chip manufacturers are exposed to many conflicting pressures from software houses and government agencies as well as privacy and user interests. As Intel discovered in relation to the serial number feature of its Pentium® III chip, implementing security features can arouse suspicion and mistrust.

Not only must the user control the chip functions, but the totality of the mechanisms used in generating keys and in writing and validating signatures (design, implementation and operation) must ensure that the owner's control of the signature can be relied on to ensure that all code approved by the owner, and only code approved by the owner, can be run. If signing processes are to be built into chips, or if chips are to run encrypted code, we need owner control of them and also publicly accountable scrutiny of the way the technical and procedural mechanisms work. Only with such scrutiny can security features gain public trust. It is particularly important that no national government can control or gain access to mechanisms which can restrict the code which users can run or which deprive users of the ability to know what functions are contained in the code their computer is running.

Call to Manufacturers

We therefore call on manufacturers of microprocessors:

- to acknowledge the principle of control by the owner;
- to permit publicly accountable scrutiny to enable the compliance of their implementations to be verified.

Acknowledgments

This Cyber-Rights & Cyber-Liberties (UK) report has been written by:

- Mr. Nicholas Bohm, E-Commerce Policy Adviser for CR&CL(UK);
- Dr Brian Gladman, Technology Policy Advisor for CR&CL(UK); and
- Mr Ian Brown, Managing Director of Cypherspace Ltd.