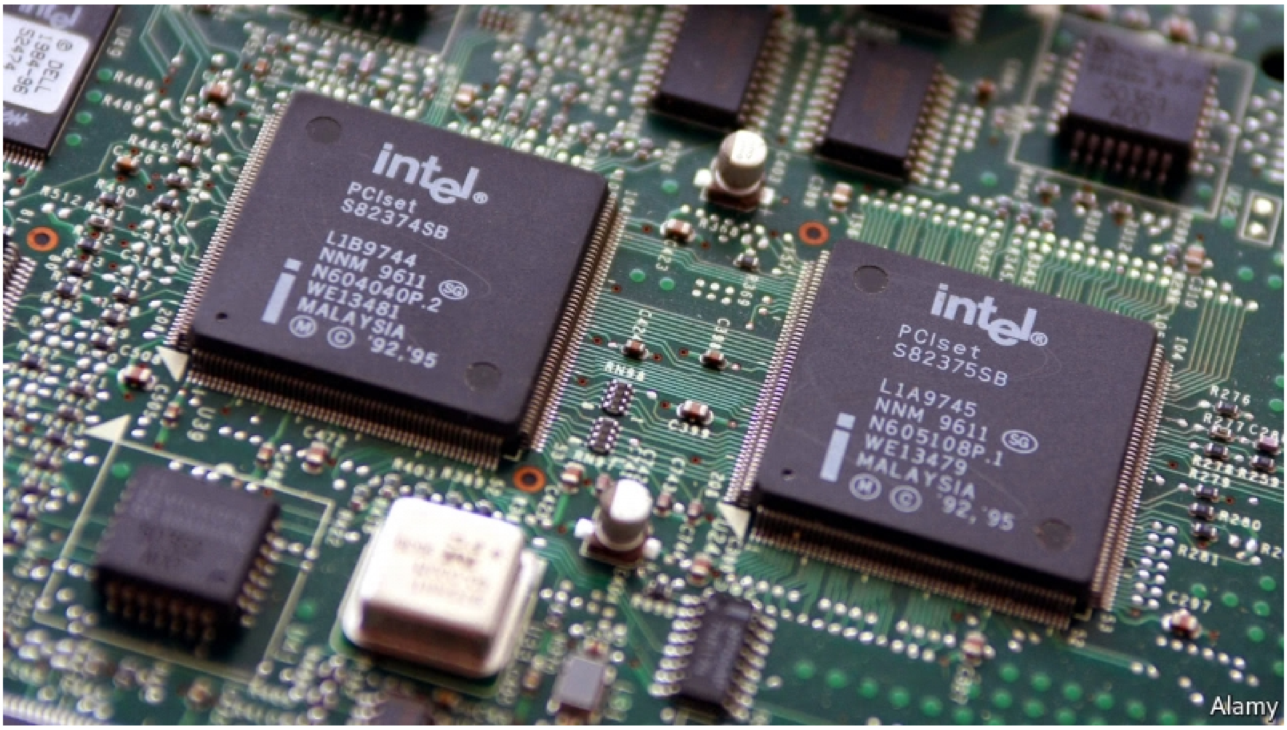
The chips are down

Two security flaws in modern chips cause big headaches for the tech business

Fixing the underlying problems will take a long time


Alamy

Science and technology Jan 4th 2018

IT WAS a one-two punch for the computer industry. January 3rd saw the disclosure of two serious flaws in the design of the processors that power most of the world's computers. The first, appropriately called Meltdown, affects only chips made by Intel, and makes it possible to dissolve the virtual walls between the digital memory used by different programs, allowing hackers to steal sensitive data, such as passwords or a computer's encryption keys. The second, dubbed Spectre, affects almost all mid-range and high-end processors in the world today. It also lets attackers open up an illicit backchannel, but in a different way: it enables a rogue program to trick a legitimate one running on the same computer to divulge information.

The double blow is unlikely to be a knock-out: big tech companies, including Apple and Microsoft, have already developed software patches to stop Meltdown, albeit at a steep cost. But neutralising Spectre will take longer, since it may well require changes in the design of the chips themselves. That means existing chips would have to be replaced by new ones, which could take years. And fixing the industry's deeper problems, which have helped create the flaws, will be harder still.

The computing industry's bottomless thirst for more processing power is at least partially to blame. Both security flaws are the result of efforts to accelerate computers that date back to the 1990s. In order to save valuable nanoseconds when running a program, processors tackle some snippets of code ahead of time, a trick called "speculative execution". Intel, the world's biggest chipmaker, seems to have taken a particularly aggressive approach, which may explain why only its chips are vulnerable to Meltdown. Because the fault lies with the chip itself, a proper software fix is not possible. Instead, Apple, Microsoft and the rest have provided patches that try to work around the problem. But one consequence is that patched Intel machines could end up running up to a third slower.

Latest updates

Visualising the careers of musicians-turned-actors
PROSPERO

How car colours reflect Britain's national sentiment
GRAPHIC DETAIL

The Czech Republic's pro-Russian president is in trouble
EUROPE

See all updates

The lack of diversity in the computing business turns such vulnerabilities into a systemic problem. Intel's chips power about 90% of personal computers and servers that sit in data centres. In the case of Spectre, although it seems to be harder to exploit, the flaw is even more widespread. Intel's chips are affected by Spectre too, but so are almost all processors from AMD and ARM, its two biggest rivals. Such chips power everything from smartphones and games consoles to desktop PCs, laptops and high-end servers.

Computers are also increasingly shared, which makes them more vulnerable to attacks. Individual machines in the data centres of Amazon Web Services, Google and other cloud-computing firms often process jobs from many customers at once. Hackers could rent capacity on them in the hope of getting information from their virtual neighbours. Unsurprisingly, these firms were quick to roll out patches for Meltdown and force customers to restart their systems.

And then there is the question of who knew about such flaws and when. Meltdown, for instance, was independently discovered by several computer-security experts a few months ago. They alerted Intel, which went to work on fixes and was planning to go public soon. That plan was scuppered when the *Register*, an online publication, found out about the flaws. But chips containing the flaws have been around for more than two decades, which raises the question of whether they have been exploited in the past, and if so by whom. Spy agencies, for instance, might have known about them for years—and used them without anybody knowing.

There are other questions. At the end of November Brian Krzanich, Intel's chief executive, sold half his shares for $14m, which left him with the minimum holding required by Intel. The transaction was executed under an automatic trading plan, but it looks bad: the plan was set up in October, after Intel got word of Meltdown. And although the firm has said that it doesn't "see any financial impact", flaws previously found in its products have been expensive: when a bug that caused its Pentium processors to divide numbers incorrectly emerged in 1994, the company took a $475m charge; a problem with a chipset in 2011 cost the firm about $700m. There are many more Intel chips in the world today than there were then. After the new flaws were disclosed, Intel's share price ended the day 3% lower than it had started it.

Do not expect quick fixes, especially for Spectre. Speculative execution is as fundamental to the working of modern chips as assembly lines are to a modern factory. Redesigning, testing and manufacturing billions of replacement devices would take years. At the same time, the economic incentives within the computing business still favour speed and sharing over security. There are good economic reasons for the lack of diversity in processors, too, chiefly the benefits of standardisation, which makes computers compatible and lowers costs. But all that also promotes brittleness and fragility. In other words, this double blow will be almost certainly be followed by other, equally painful ones.

Correction (January 5th 2018): *Speculative execution, which is explained in the third paragraph, saves nanoseconds, not milliseconds.*