Trust in tech

As the world of connected devices continues to expand, the need to develop more secure technology becomes increasingly relevant.

At the start of this year, it was announced that two security flaws — known as Spectre¹ and Meltdown² — had been identified in the microprocessors used in many of the world's computers. The flaws take advantage of a feature of modern central processing units (CPUs) known as speculative execution. Here the CPU, in order to improve performance, guesses what tasks might be needed: if wrong, the speculative execution is discarded, but if correct, work has already been done and time is saved. By exploiting the way data is protected during such processes, Spectre and Meltdown could potentially allow an attacker to access confidential information in the memory, including the kernel memory, of a device.

The vulnerabilities affect chips from Intel, AMD and ARM, and software patches have been issued. But, ultimately, more radical solutions might be required³. The question of how to ensure the security of devices is also becoming increasingly pressing as the Internet of Things develops, and chips find their way into a variety of everyday objects. However, there are some emerging possibilities. For a start, there are ongoing efforts to develop security-focused computer architectures⁴, such as the Capability Hardware Enhanced RISC Instructions (CHERI) architecture from researchers at the University of Cambridge and SRI International, which can isolate malicious software⁵.

These architectural approaches still work with conventional complementary metal–oxide–semiconductor (CMOS) technology. By considering changes at a more fundamental level, novel forms of security hardware can also be developed. Memristors have, in particular, recently emerged as devices well suited for use as security primitives⁶, and in the application of digital keys, due to the intrinsic variations in their switching characteristics.

Mechanical lock and key devices have been in use for thousands of years, and their digital equivalents are an essential component of security in electronic systems today. These digital keys, through encryption and authentication, guard against unauthorized access. Information transported over a network can, for example, be protected through encryption with a key known to just the sender and the intended recipients. Alternatively, when the fabrication of a chip is outsourced to an external foundry, the chip can be protected from intellectual

Optical image of a 128 × 64 memristor crossbar array. Credit: reproduced from ref.⁸, Springer Nature Ltd

property theft or unauthorized production by incorporating key gates (extra logic gates). Known as logic locking⁷, these gates will stop the chip from working properly unless they are unlocked by a key known only to the chip designer. There is, though, an issue with such an approach: once a device has a key, it can be hard to remove it, and to know that it has, in fact, been removed.

In an Article in this issue of *Nature Electronics*, J. Joshua Yang, Daniel Holcomb, Qiangfei Xia and colleagues at the University of Massachusetts, Amherst show that memristor crossbar arrays can provide a physical fingerprint that proves that a digital key stored in the array has been securely destroyed⁸. The fingerprint is generated by comparing the conductance of neighbouring memristor cells when they are in a low-resistance state. The key,

which can unlock the capabilities of the chip, is stored in the crossbar array over the memristor fingerprint. To reveal the fingerprint, the digital key has to be erased. The approach is illustrated using a 128 × 64 hafnium oxide memristor crossbar array, and the researchers also devise a protocol for implementing the provable key destruction scheme in chip logic locking and unlocking.

As Wenjie Xiong and Jakub Szefer of Yale University note in an accompanying News & Views article in this issue: “Traditional cryptographic approaches base security on the hardness of mathematical problems. The approach adopted by Xia and colleagues is distinct, as the security lies in the uniqueness of the physical properties of memristive devices in a crossbar array configuration.”

Questions of security also raise questions about trust. And the multitude of issues that surround trust and technology in our connected age is something that the recently launched Trust & Technology Initiative at the University of Cambridge sets out to explore. Through an interdisciplinary approach, the initiative aims to help develop internet technologies that work well for society. On one level this involves the development of secure computer systems. But it also requires an understanding of the relationship between society and technology (not to mention the organizations that make it), as well as an understanding of the very nature of trust in this context. Such endeavours are a valuable addition in the pursuit of secure, and trustworthy, technology for all. □

Published online: 12 October 2018
<https://doi.org/10.1038/s41928-018-0159-0>

References

1. Kocher, P. et al. Preprint at <https://arxiv.org/abs/1801.01203> (2018).
2. Lipp, M. et al. Preprint at <https://arxiv.org/abs/1801.01207> (2018).
3. Hachman, M. Solving Spectre and Meltdown may ultimately require an entirely new type of processor. *PCWorld* (21 August 2018); <https://go.nature.com/2bwhBvd>
4. Adee, S. Uncrackable computer chips stop malicious bugs attacking your computer. *New Scientist* (8 August 2018); <https://go.nature.com/2Qpmrx9>
5. Watson, R. N. M., Woodruff, J., Roe, M., Moore, S. W. & Neumann, P. G. Capability Hardware Enhanced RISC Instructions (CHERI): Notes on the Meltdown and Spectre Attacks UCAM-CL-TR-916 (Univ. Cambridge, 2018); <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-916.pdf>
6. Nili, H. et al. *Nat. Electron.* **1**, 197–202 (2018).
7. Roy, J. A., Koushanfar, F. & Markov, I. L. *Computer* **43**, 30–38 (2010).
8. Jiang, H. et al. *Nat. Electron.* <https://doi.org/10.1038/s41928-018-0146-5> (2018).