**PRACTICALLY EVERY WORD** we use to describe a computer is a metaphor. "File,” “window,” even “memory” all stand in for collections of ones and zeros that are themselves representations of an impossibly complex maze of wires, transistors and the electrons moving through them. But when hackers go beyond those abstractions of computer systems and attack their actual underlying physics, the metaphors break.

Over the last year and a half, security researchers have been doing exactly that: honing hacking techniques that break through the metaphor to the actual machine, exploiting the unexpected behavior not of operating systems or applications, but of computing hardware itself---in some cases targeting the actual electricity that comprises bits of data in computer memory. And at the Usenix security conference earlier this month, two teams of researchers presented attacks they developed that bring that new kind of hack closer to becoming a practical threat.

**Breaking Assumptions**

Both of those new attacks use a technique Google researchers [first demonstrated last March called "Rowhammer."](https://www.wired.com/2015/03/google-hack-dram-memory-electric-leaks/) The trick works by running a program on the target computer, which repeatedly overwrites a certain row of transistors in its DRAM flash memory, “hammering” it until a rare glitch occurs: Electric charge leaks from the hammered row of transistors into an adjacent row. The leaked charge then causes a certain bit in that adjacent row of the computer's memory to flip from one to zero or vice versa. That bit flip gives you access to a privileged level of the computer's operating system.

It's messy. And mind-bending. And it works.

Rowhammer and similar attacks could require both hardware and software makers to rethink defenses based on purely digital models. "Computers, like all technologies really, are built in layers that make assumptions of one another. Think of a car, assuming its wheels roll and absorb shocks, and don't melt into goop when they get wet," says security researcher Dan Kaminsky, who found a fundamental flaw in the Internet's domain name system in 2008. "What’s interesting about networked technology is the fact that those assumptions can be attacked."

Last year, Thomas Dullien (one of the inventors of the technique, perhaps better known by his hacker handle Halvar Flake) and his fellow Google researchers showed that they could use electricity leakage to flip crucial bits in the DRAM memory of a set of laptops, the first proof that charge leakage could be predictable and exploitable. Researchers in Austria and France [followed up a few months later](http://arxiv.org/pdf/1507.06955v1.pdf) to show the attack could be enabled by javascript code running in a browser.

Those variations on Rowhammer, along with the newest ones presented at Usenix, show that the hacker world is increasingly focused on techniques that break those fundamental assumptions of computing. "Rowhammer is just scratching the surface," says Dullien. "This has the potential to be a gigantic field of research."

**Making Rowhammer Practical and Specific**

The latest attacks take Rowhammer in a new direction, applying it to cloud computing services and enterprise workstations rather than consumer PCs. One [attack by a group of Ohio State researchers](https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_xiao.pdf) used the technique to hack Xen, the software used to partition computing resources on cloud servers into isolated "virtual machines" rented to customers. The hack breaks out of those virtual machines to control deeper levels of the server.

A [second paper](https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_razavi.pdf) by Dutch and Belgian researchers achieves a similar effect, and also shows a new way to use Rowhammer more reliably. It exploits a feature called "memory de-duplication" that combines identical parts of virtual machines' memory into a single place in the memory of a physical computer. On the Dell workstation the researchers tested, they could write data into the memory of a virtual machine and then use that data to locate and "hammer" the physical transistors underlying not just those bits of data, but the identical bits on someone else's virtual machine running on the same computer.

TRENDING NOW

**[Hacking Police Body Cameras](https://www.wired.com/video/watch/hacking-police-body-cameras" \l "intcid=_cne-interlude-wired_3094895f-1359-4ba5-8d8a-15b063e0eea7_text2vec1" \t "_blank)**

The trick, which the researchers call "Flip Feng Shui," allowed the group to pull off highly targeted hacks, like sabotaging an encryption key so that they could later decrypt a target's secrets. "It’s less like a flamethrower and more like a sniper rifle," says Ben Gras, one of the researchers at the University of Vrije who came up with it.1

**A New Level of Stealth**

Rowhammer is far from the only new hacking technique that exploits computers' physical properties. Proof-of-concept malware shown off by Israeli researchers over the summer, for instance, uses the sound of [computers' cooling fans](https://www.wired.com/2016/06/clever-attack-uses-sound-computers-fan-steal-data/) or [hard drive motors](http://arstechnica.com/security/2016/08/new-air-gap-jumper-covertly-transmits-data-in-hard-drive-sounds/) to transmit stolen data as audio. Another group of Israelis showed last year they could use just $300 of handheld equipment to [extract encryption keys from a computer by monitoring the radio emissions leaked by its processor's power use](https://www.wired.com/2015/06/radio-bug-can-steal-laptop-crypto-keys-fits-inside-pita/).

**The result is an ultra-stealthy physical sabotage technique that's virtually impossible to detect with digital security measures.**

But as with Rowhammer, the most disturbing physical hacks are microscopic. University of Michigan researchers have been able to build a secret backdoor into a single cell---a collection of transistors less than a thousandth of the width of a human hair---among billions on a modern microchip. When a hacker who knows about the backdoor's existence runs a certain program, it causes that cell to pick up charge from nearby transistors and induce a certain bit to flip, just as in the Rowhammer attacks. The result is an ultra-stealthy physical sabotage technique that's virtually impossible to detect with digital security measures. "It's operating outside of the Matrix," says Matthew Hicks, one of the Michigan researchers, [who described the technique to WIRED in June](https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/).

This kind of exploitation of hardware means that no software update can help. Researchers have identified one countermeasure to Rowhammer's memory charge leakage: a feature of DRAM called "error-correcting code" constantly corrects abnormal levels of charge in any particular transistor. More widely implementing that feature in computer memory could head off current implementations of the Rowhammer attack.

But Dullien warns that DRAM is just one potential target. "Lots of things---chips, hard disks, whatever---are designed to be OK in the average case but probably not when they're given adversarial input," he says. "We don’t know where the next broken piece of hardware will show up. But that's why everyone’s so excited about researching this more." Computer scientists may soon find their machines aren’t just vulnerable in ways they haven’t considered, but in ways their digital models don't even allow them to imagine.