DOI:10.1145/1506409.1506428

Technical Perspective
A Chilly Sense of Security

By Ross Anderson

THE FOLLOWING PAPER by Alex Halderman et al. will change the way people write and test security software.

Many systems rely on keeping a master key secret. Sometimes this involves custom hardware, such as a smartcard, and sometimes it relies on an implicit hardware property, such as the assumption that a computer's RAM loses state when it is powered off. And software writers tend to assume that hardware works in the intuitively obvious ways.

But technological progress can undermine old assumptions.

Years ago, Sergei Skorobogatov showed that memory cells used in microcontrollers could retain their contents for many minutes at low temperatures; an attacker could freeze a chip to stop its keys evaporating while he depackaged it and probed out the contents.

That was long thought to be an arcane result of relevance only to engineers designing crypto boxes for banks and governments. But, as this paper illustrates, progress has made memory remanence (as it is known) relevant to the "ordinary" software business, too. Modern memory chips, when powered down, will retain their contents for seconds even at room temperature, and for minutes if they are cooled to the temperatures of a Canadian winter.

The upshot is that your laptop encryption software is no longer secure.

The key used to protect disk files is typically kept in RAM, so a locked laptop can be unlocked by cooling it, interrupting the power, rebooting with a new operating system kernel, and reading out the key.

Even if a few bits of the key have decayed, common implementations of both DES and AES keep redundant representations of the key in memory to improve performance; these not only provide error correction but enable keys to be found quickly.

This neat piece of work emphasizes once more the need for engineers who build security applications to take a holistic view of the world.

For their pièce de résistance, the authors show how to break BitLocker, the disk encryption utility in Microsoft Vista, and the culmination of the 10-year, multibillion-dollar "Trusted Computing" research program. BitLocker was believed to be strong because the master keys are kept in the TPM chip on the motherboard while the machine is powered down. Hundreds of millions of PCs now have TPM chips; your PC cost a few dollars more as a result. But did it make your PC more secure? It turns out that keys remain in memory so long as the machine is powered up; and worse, they are loaded to memory when the machine is powered on, before the user ever has to enter a password. In either case, the memory remanence attack can suck them up just fine. The upshot is that you're less secure than before. An old-fashioned disk encryption utility can at least protect your data when your machine is powered down. Adding "hardware security" has undermined even that.

This neat piece of work emphasizes once more the need for engineers who build security applications to take a holistic view of the world.

Software alone is not enough; you need to understand the hardware, and the people too.

Ross Anderson (Ross.Anderson@cl.cam.ac.uk) is a professor of security engineering at the University of Cambridge, England.