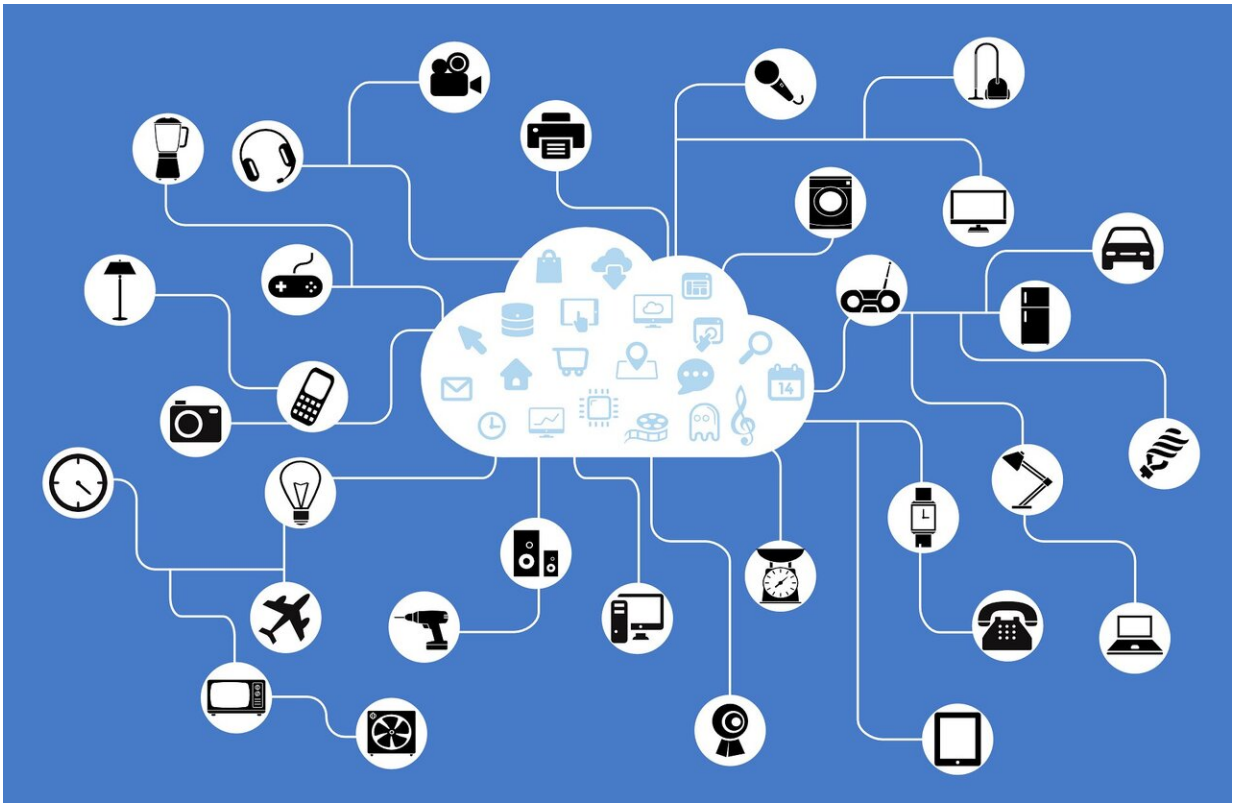
A fingerprint for the Internet of Things

September 17 2020, by Tom Jeltes



Credit: Pixabay/CC0 Public Domain

The Internet of Things (IoT) consists of billions of sensors and other devices connected to each other via internet, all of which need to be protected against hackers with malicious purposes. A low-cost and energy efficient solution for the security of IoT devices uses the unique characteristics of the built-in memory chips. Ph.D. candidate Lieneke

Kusters investigated how to make optimal use of the chip's digital fingerprint to generate a security key.

The higher the number of devices connected to each other via the Internet of Things, the greater the risk that malicious hackers might gain access to important information, or even take over entire systems. Quite apart from all kinds of privacy issues, it's not hard to imagine that that someone who, for example, has control over temperature sensors in a chemical or nuclear plant, could cause serious damage.

To prevent problems like these from occurring, each IoT device needs to be able, as it were, to show an identity document—"authentication," in professional terms. Normally, speaking, this is done with a kind of password, which is sent in encrypted form to the person who is communicating with the device. The security key needed for that has to be stored in the IoT device one way or another, Lieneke Kusters explains. "But these are often small and cheap devices that aren't supposed to use much energy. To safely store a key in these devices, you need extra hardware with constant power supply. That's not very practical."

Digital fingerprint

There is a different way: namely by deducing the security key from a unique physical characteristic of the memory chip (Static Random-Access Memory, or SRAM) that can be found in practically every IoT device. Depending on the random circumstances during the chip's manufacturing process, the memory locations have a random default value of 0 or 1.

"That binary code, which you can read out when activating the chip, constitutes a kind of digital fingerprint of the device," says Kusters, who gained her doctorate at the Information and Communication Theory

Laboratory at the TU/e department of Electrical Engineering. This fingerprint is known as a Physical Unclonable Function (PUF). "The Eindhoven-based company Intrinsic ID sells digital security based on SRAM-PUFs. I collaborated with them for my doctoral research, during which I focused on how to generate, in a reliable way, a key from that digital fingerprint that is as long as possible. The longer, the safer."

The major advantage of security keys based on SRAM-PUFs is that the key exists only at the moment when authentication is required. "The device restarts itself to read out the SRAM-PUF and in doing so creates the key, which subsequently gets erased immediately after use. That makes it all but impossible for an attacker to steal the key."

Noise and reliability

But that's not the entire story, because some bits of the SRAM do not always have the same value during activation, Kusters explains. Ten to fifteen percent of the bits turn out not to be determined, which makes the digital fingerprint a bit fuzzy. How do you use that fuzzy fingerprint to make a key of the highest possible complexity that nevertheless still fits into the receiving lock—practically—each time?

"What you want to prevent is that the generated key won't be recognized by the receiving party as a consequence of the 'noise' in the SRAM-PUF," Kusters explains. "It's alright if that happens one in a million times perhaps, preferably less often." The probability of error is smaller with a shorter key, but such a key is also easier to guess for people with bad intentions. "I've searched for the longest reliable key, given a certain amount of noise in the measurement. It helps if you store extra information about the SRAM-PUF, but that must not be of use to a potential attacker. My thesis is an analysis of how you can reach the optimal result in different situations with that extra information."