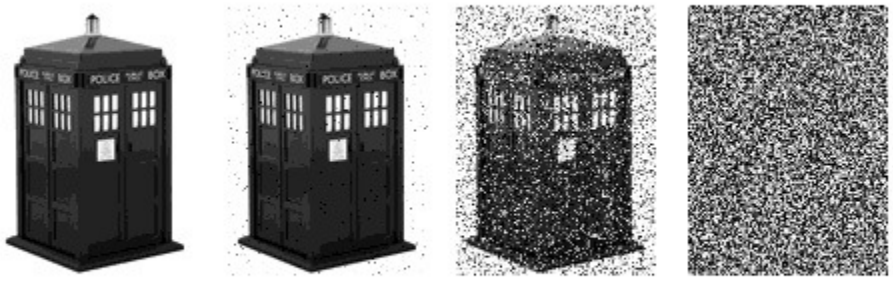
New technology for better security of RFID chips without any additional hardware



" All images used are for illustrative purposes only. The material available on this website is provided for general information and education purposes only. All images are copyrighted by their respective owners "

Data (like this picture) stored in an RFID chip's SRAM decays. This technology uses that decay as a clock that tells when the chip last received power

A Research Organization has developed a new technology for better security of RFID chips by creating a short-duration "clock" on batteryless radio-frequency identification (RFID) chips, rendering their cryptographic systems much less vulnerable to attack.

The clock operates over spans of seconds to minutes after an RFID chip is charged up from an RFID reader or other ambient radio-wave energy. As a result, even after the radio signal is removed, the clock endows the RFID chip with the ability to know when its security keys may be in danger.

The researchers are using this circuit in a way that was designed to be memory, but they're turning it into what's effectively an hourglass.

The researchers says the inspiration for the discovery came from the studies while exploring the properties of static RAM (SRAM), the main memory in microprocessors and a kind that loses its data when the power is off. They discovered that powered-down SRAM decays from its powered-up state in predictable patterns. If you gather enough SRAM bits, the group discovered, the statistics of the memory's decay to its zero-power state enables it to be used as an ersatz hourglass.

Having a clock can be very useful in defending against brute-force attacks that may try to guess the chip's passwords hundreds or thousands of times per second. The technology-enabled chip—requiring no new hardware and representing fewer than 50 lines of additional code—would receive a power-up from, say, a nearby RFID reader. Instead of wiping the SRAM clean, the device would first read off the state of the SRAM, which would be partially decayed from the last time the chip was powered up. Comparing the percentage of decayed bits to a precompiled table would enable this new technology to read off the time elapsed since the previous power-up.

How does that help? “There are different kinds of attacks, but all of them involve repeated, multiple accesses. And the more you can access this thing quickly, the higher your chances are to crack it.”

If the time that this new technology detects is seconds or more, the chip is probably safe. But if the time between power-ups is just milliseconds, and there have been many failed attempts to communicate with the chip within recent memory, then this new technology would conclude the chip may be under attack.

Unlike cruder present-day RFID defense measures—such as France’s e-passports that punish every successive failed RFID read with an increasingly longer lag, causing frustrating wait times for travelers and customs officials— this new technology would theoretically permit standard occasional communications but severely constrain the tsunami of failed attempts that are the hallmark of a hostile attack.

The phenomenon of SRAM remanence is usually seen as a chip weakness that must be defended: Attackers may conceivably be able to read off some bits from a chip after its power shuts down. But this is one of the first cases of which the researchers are aware of where SRAM remanence is a good thing.

Battery- or capacitor-powered clocks might achieve the same end, but adding them to an RFID chip that costs 5 U.S. cents would be too pricey, this new technology represents a smart, zero-cost solution.

We need to be ahead of the curve and not wait for everybody’s smart credit cards to be cracked, the companies that are going to put out RFID cards are going to need assurances that these things are safe. So this new technology is more of a necessary condition for RFID applications to really take off.”

For Additional Information please contact info@technologyconcepts.in