Short-duration clock approach thwarts RFID attacks

August 7 2012, by Nancy Owano

(Phys.org) -- Security researchers and practitioners at the 21st USENIX Security Symposium in Bellevue, Washington, which starts on Wednesday, will learn how researchers have devised an hourglass technology that can thwart attacks by RFID thieves. The study, by researchers from University of Massachusetts Amherst; University of California, Berkeley; and Dartmouth College, will be presented at the event, their work involves the use of a short-duration “clock” on batteryless radio-frequency identification (RFID) chips—that means no special-purpose hardware needed. The idea is to reduce vulnerability to attacks.

TARDIS stands for Time And Remanence Decay in SRAM. The

attractiveness of the approach lies not only in efficacy but in simplicity. A TARDIS-enabled chip does not require hardware and represents fewer than 50 lines of additional code. The chip can get a power-up from an RFID reader nearby. 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 TARDIS to read off the time elapsed since the previous power-up. 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. Even after the radio signal is removed, the clock lets the RFID chip know when its security keys may be in danger. A clock of this nature is a way to defend against the type of brute-force attacks that try to guess the chip's passwords hundreds or thousands of times per second.

The paper of the same name "Time And Remanence Decay in SRAM" will be presented at the Bellevue gathering. In a preview report in IEEE Spectrum, Kevin Fu, Associate Professor of Computer Science at the University of Massachusetts Amherst, and part of the research effort, commented on the short-duration clock technique that will be presented on Wednesday at USENIX. "We're using this circuit in a way that was designed to be memory, but we're turning it into what's effectively an hourglass," he said.

The TARDIS researchers were motivated to do their study based on the lack of a locally trustworthy clock that makes security protocols challenging to implement on batteryless embedded devices such as contact smartcards, contactless smartcards, and RFID tags. They noted that a device which knows how much time has elapsed between queries from an untrusted reader could better protect against attacks that depend on the existence of a rate-unlimited encryption oracle.

According to their paper, "The TARDIS enables coarse-grained,

hourglass-like timers such that cryptographic software can more deliberately decide how to throttle its response rate."

The TARDIS consists purely of software, making the mechanism easy to deploy on devices with SRAM. Outside of the TARDIS team, academics have been weighing in on this research. While battery- or capacitor-powered clocks might achieve the same end, Srini Devadas, a professor of electrical engineering and computer science at MIT, noted the cost difference. Adding them to an RFID chip that costs five U.S. cents would be too pricey. TARDIS, he says, represents a smart, zero-cost solution.