Poster: TARDIS
Secure Time Keeping For Embedded Devices Without Clocks

Amir Rahmati
UMass Amherst

Mastooreh Salajegheh
UMass Amherst

Dan Holcomb
UC Berkeley

Jacob Sorber
Dartmouth College

Wayne Burleson
UMass Amherst

Kevin Fu
UMass Amherst

1 Introduction

Lack of a locally trustworthy clock makes security protocols challenging to implement on batteryless embedded devices such as contact smartcards, contactless smartcards, and RFID tags. A device that 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.

The TARDIS (Time and Remanence Decay in SRAM) helps to locally maintain a sense of time elapsed without power and without special-purpose hardware. The TARDIS software computes the expiration state of a timer by analyzing the decay of existing on-chip SRAM memory. The TARDIS enables coarse-grained, hourglass-like timers such that cryptographic software can more deliberately decide how to throttle its response rate. Our experiments demonstrate that the TARDIS can measure time ranging from seconds to several hours depending on hardware parameters.

In this work we will discuss SRAM decay and how it can be used to acquire a notion of time. We will also present our evaluation results and how TARDIS can be used in different applications.

2 TARDIS

To enable security protocols on intermittently powered devices without clocks, we propose Time and Remanence Decay in SRAM (TARDIS) to keep track of time without a power source and without additional circuitry. The TARDIS relies on the behavior of decaying SRAM circuits to estimate the duration of a power failure (Figure 1). Upon power-up, the TARDIS initializes a region in SRAM of a intermittently powered device. Later, during power-off, the SRAM memory starts to decay. Upon the next power-on, the TARDIS measures the fraction of SRAM cells that retain their state.

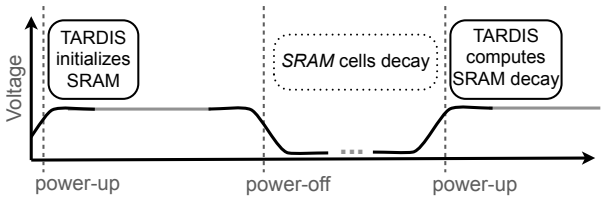

Figure 1: TARDIS estimates time by counting the number of SRAM cells that their value at power-up is zero (*computes SRAM decay*). Initially, a portion of SRAM cells are set to one (*initializes SRAM*) and their values decay during power-off. The dots in the power-off indicate the arbitrary and unpredictable duration of power-off.

Three distinct stages of decay are observed in all experiments. Figure 2 illustrates the three stages of SRAM decay measured on a TI MSP430F2131 with 256 Bytes of RAM and a $10\mu F$ capacitor, at $26^{\circ}C$. We vary the *off-time* from 0 to 400 seconds in 20-second increments. In the first stage, no memory cells have decayed; during the second stage, a fraction of the cells, but not all, have decayed; and by the third stage the cells have decayed completely. Observations made during stages 1 or 3 provide a single bit of coarse information, indicating only that stage 2 has not yet begun or else that stage 2 has already been completed. Observations made during stage 2 can provide a more accurate notion of time based on the percentage of decayed bits.

3 Applications

Unawareness of time has left contactless payment cards vulnerable to a number of successful attacks (Table 1). For instance, Kasper et al. [7] recently demonstrated how to extract the 112-bit key from a MIFARE DESFire contactless smartcard (used by the Clipper all-in-one transit payment card). The side channel attack required approx-

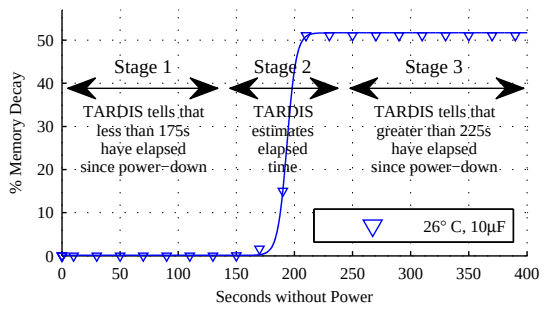

Figure 2: The TARDIS presents a three stage response pattern according to its amount of decay. Before 175 seconds, the percentage of bits that retain their 1-value across a power-off is 100%. For times exceeding 225 seconds, the TARDIS memory has fully decayed. The decay of memory cells between these two thresholds can provide us with a more accurate measurement of time during that period.

Platform	Attack	#Queries
MIFARE Classic	Brute force [3]	$\geq$1,500
MIFARE DESFire	Side channel [7]	250,000
UHF RFID tags	Side channel [6]	200
TI DST	Reverse eng. [1, 2]	$\sim$75,000
GSM SIM card	Brute force [4]	150,000

Table 1: Practical attacks on intermittently powered devices. These attacks require repeated interactions between the reader and the device. Throttling the reader attempts to query the device could mitigate the attacks.

imately 10 queries/sec for 7 hours. Some RFID credit cards are vulnerable to replay attacks due to lack of a notion of time [5]. Oren and Shamir [6] show that power analysis attacks on UHF RFID tags can recover the password protecting a "kill" command with only 200 queries. At USENIX Security 2005, Bono et al. [2] implemented a brute-force attack against the Texas Instruments Digital Signature Transponder (DST) used in engine immobilizers and the ExxonMobile SpeedPass™. The first stage of the attack required approximately 75,000 online "oracle" queries to recover the proprietary cipher parameters [1].

A batteryless device could mitigate the risks of brute-force attacks, side-channel attacks, and reverse engineering by throttling its query response rate. However, the tag has no access to a trustworthy clock to implement throttling. A smartcard does not know whether the last interrogation was 5 seconds ago or 5 days ago. TARDIS empowers these devices with a sense of time, enabling them to preform throttling. TARDIS can also be used to implement time out for query response and prevent pass back and double reads.

4 Conclusion

In this work we introduced the TARDIS; A trustworthy source of time on batteryless devices that could enable cryptographic protocols to more deliberately defend against semi-invasive attacks such as differential power analysis and brute force attacks. The TARDIS uses remanence decay in SRAM to compute time elapsed during a power outage—ranging from seconds to hours depending on hardware parameters. The mechanism provides a coarse-grained notion of time for intermittently powered computers that otherwise have no effective way to measure time. Applications using the TARDIS primarily rely on timers with hourglass-like precision to throttle queries. The TARDIS consists purely of software—making the mechanism easy to deploy on devices with SRAM. A novel aspect of the TARDIS is its use of memory decay or data remanence for improved security rather than attacking security.

References

[1] BONO, S., February 2012. Personal communication.

[2] BONO, S. C., GREEN, M., STUBBLEFIELD, A., JUELS, A., RUBIN, A. D., AND SZYDLO, M. Security analysis of a cryptographically-enabled RFID device. In *Proceedings of the 14th conference on USENIX Security Symposium - Volume 14* (2005), USENIX Association, pp. 1–1.

[3] GARCIA, F. D., ROSSUM, P. V., VERDULT, R., AND SCHREUR, R. Wirelessly pickpocketing a Mifare Classic card. In *IEEE Symposium on Security and Privacy* (May 2009), pp. 3 –15.

[4] GOLDBERG, I., AND BRICENCO, M. GSM cloning. `http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html`, 1999. Last Viewed February 19, 2012.

[5] HEYDT-BENJAMIN, T. S., BAILEY, D. V., FU, K., JUELS, A., AND OHARE, T. Vulnerabilities in first-generation RFID-enabled credit cards. In *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 4886* (Lowlands, Scarborough, Trinidad/Tobago, February 2007), pp. 2–14.

[6] OREN, Y., AND SHAMIR, A. Remote password extraction from RFID tags. *Computers, IEEE Transactions on 56*, 9 (sept. 2007), 1292 –1296.

[7] OSWALD, D., AND PAAR, C. Breaking mifare desfire mf3icd40: Power analysis and templates in the real world. In *CHES* (2011), pp. 207–222.