SRAM-based Physical Unclonable Keys for BLE Smart Lock Systems

Miguel A. Prada-Delgado, Alfredo Vázquez-Reyes,
Iluminada Baturone
Instituto de Microelectrónica de Sevilla (IMSE-CNM)
University of Seville – CSIC. Seville, Spain
{prada, vazquez, lumi}@imse-cnm.csic.es

Laurentiu Acasandrei, Diego Fernández-Barrera,
Javier Prada-Delgado
OCLOSE S.L.
Seville, Spain
{lau, diego, javier}@oclose.com

***Abstract*— Nowadays, several smart lock systems use Bluetooth Low Energy (BLE) to recognize when a smartphone, conveniently authenticated by a digital key, is near. The keys can be shared and are managed by web apps, so that system security depends on how the software prevents an attacker from discovering the keys. In order to increase security by a two-factor method ('something you have' in addition to 'something you know'), the BLE smart lock system prototype shown in this demonstrator recognizes when a user wearing an authenticated BLE chip (in a key fob, wristband, etc.) is near. The digital keys are not stored but they are regenerated on the fly by only the trusted chip. This is possible by using the start-up values of the SRAM in the BLE chip, which acts as a physical unclonable function (PUF), so that the chip cannot be cloned. The SRAM start-up values of the BLE chip are also exploited as true random numbers to derive fresh keys for each transaction with the lock.**

Keywords*— *secure systems, hardware security, PUFs, TRNGs

I. Summary

Smart lock systems are being installed in houses, cars, lockers and boxes for postal applications, logistic solutions, storage, etc. The systems considered in this demonstrator are based on Bluetooth Low Energy (BLE), which is a very suitable protocol for communication with small and power constrained hardware such as the physical key (which can be a wristband, card, etc. containing a BLE chip). The physical keys employed for this demonstrator are the key fobs from Texas Instruments that contain a CC2541 BLE chip and operate on a single coin cell battery. The upper part of Figure 1 illustrates the components of the smart lock system.

The usual security features of a BLE connection are that digital keys are sent wirelessly, which can suffer from man-in-the-middle attacks, or that a passcode stored in the code is used to create the digital key, which can be copied by an attacker. In the solution presented in this demonstrator, the digital keys are not stored in the code or transmitted. The BLE chip of each physical key is bound to its code because the data (helper data) stored in its code only allows it to create the digital key. If the code is copied and executed in another key fob with another BLE chip, the digital key cannot be reconstructed. The code associated to each key fob is created during a registration phase in which the unique helper data are obtained from the start-up values of the SRAM in the CC2541 chip and from the digital key shared by the key fob and the lock. The bottom part of Figure 1 illustrates the small Hamming distances between SRAM responses generated by the same CC2541 BLE chip at different start-ups (histogram in green on the left) and the higher distances when the responses are generated by other chips (histogram in red on the right). Genuine and impostor key fobs are distinguished robustly by processing SRAM responses adequately [1]-[2]. Data stored in the code do not reveal anything about the digital key because the SRAM start-up values are unbiased previously to generate the helper data [3]. If the key fob is powered up, the start-up values of the non-initialized SRAM cells are read to recover the shared digital key and to generate random numbers that will be employed to derive fresh digital keys to encrypt and authenticate the link with the lock, thus avoiding replay attacks [1]-[2].

This work was partially supported by TEC2014-57971-R and RTC-2014-2932-8 projects from the Spanish Government (Ministerio de Economía y Competitividad) with support from FEDER. M. A. Prada-Delgado is supported by 'V Plan Propio de Investigación' from the University of Seville.

References

[1] I. Baturone, M.A. Prada-Delgado, S. Eiroa, "Method and device to generate identifiers and true random numbers", Patent Application, Priority Number P201400225, 2014.

[2] I. Baturone, M.A. Prada-Delgado, S. Eiroa. "Improved generation of identifiers, secret keys, and random numbers from SRAMs", IEEE Trans. on Inform. Forensics and Security, pp. 2653–2668, Dec. 2015.

[3] R. Maes, V. van der Leest, E. van der Sluis, F. Willems, "Secure key generation from biased PUFs", Proc. Cryptographic Hardware and Embedded Systems, CHES 2015, vol. 9293 of LNCS, pp 517-534.

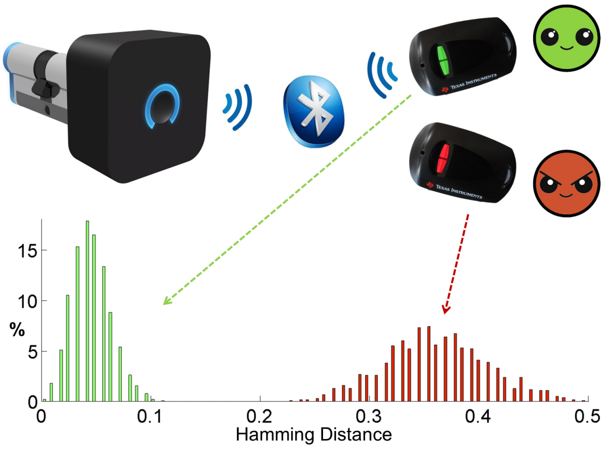

Fig. 1. The lock and key fobs in the smart lock system. The genuine and impostor key fobs are distinguishable.