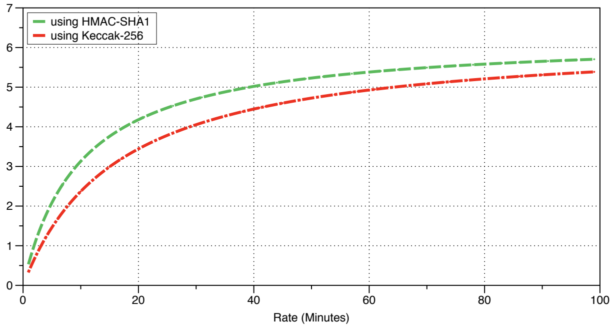

Figure 4: The impact on battery lifetime when using either HMAC-SHA1 or Keccak-256 primitives in SPEED.

of this party. We measure according to the speed of the light. So, a delay of 1 *ns* affects the distance of 15 cm. The microcontroller between hands (e.g. ATmega 1284p) operates on 10 MHz frequency and this means having a resolution of 100 *ns* in the ideal condition (e.g. The processing time is identified accurately on both sides, etc.), where a device with a distance of 1 *m* is detected as 15 *m* farther. Longer the range the more accurate is the measurement. For example, with this resolution, all devices within a range of 1 *m* to 14 *m* will be labeled with a distance of around 15 *m*. Since we are conducting our experiment within close range, this resolution does not help us. Therefore, we depend on the distance measurement functionality in the transceiver module itself. The IEEE 802.15.4 transceiver [5] between hands has a *time-of-flight* facility built into the hardware that improves the accuracy of measuring distance. Experimentally, we got an accuracy of 3 meters, which means a resolution of 20 *ns*. However, there are some distance measurement technologies [13] that integrate the aforementioned transceiver with a custom firmware to acquire special features like a RADAR system, thus giving a high accuracy where the resolution is near 1 *ns*.

Nevertheless, not all microcontrollers are integrated with such type of transceivers. In this case, the microcontroller should rely on the internal capabilities to calculate RTT accurately. Though recent work has yielded some proposals for establishing the upper bound on the distance between wireless sensor nodes with standard hardware [2], we still believe that this research problem is hardware-dependent and remains an open issue.

8 CONCLUSION & FUTURE WORK

Secure remote decommissioning (e.g. erasure) is as important as secure remote provisioning (e.g. deployment), and should be a key requirement for IoT devices. This paper proposed SPEED, an approach to secure provable erasure for embedded devices. It can be applied to all Class-1 IoT devices without any limitations. Our approach depends on isolating part of the flash memory using selective software virtualization and assembly level verification to store the trusted software module. We then build the secure erasure mechanism using DB protocol to prevent man-in-the-middle attack. The evaluation results show that SPEED incurs an acceptable overhead in terms of memory footprint, power consumption and performance. A fundamental limitation of SPEED is that it is limited to small (visual) distances.

In future work, we plan to investigate SPEED with a stronger attacker model where physical attack (e.g. the invasive one) should be taken into account by implementing some techniques in the TSM to detect it (e.g. detecting loss of power). Finally, a formal verification of the TSM code and a demonstration of a real and complete scenario including secure software deployment as well is another future goal.

REFERENCES

[1] Tigist Abera, N Asokan, Lucas Davi, Farinaz Koushanfar, Andrew Paverd, Ahmad-Reza Sadeghi, and Gene Tsudik. 2016. Things, trouble, trust: on building trust in IoT systems. In *Proceedings of the 53rd Annual Design Automation Conference.* ACM, 121.

[2] Stephan Adler, Stefan Pfeiffer, Heiko Will, Thomas Hillebrandt, and Jochen Schiller. 2012. Measuring the distance between wireless sensor nodes with standard hardware. In *Positioning Navigation and Communication (WPNC), 2012 9th Workshop on.* IEEE, 114–119.

[3] Muneeb Ahmad, Jalal S Alowibdi, and Muhammad U Ilyas. 2017. vIoT: A first step towards a shared, multi-tenant IoT Infrastructure architecture. In *Communications Workshops (ICC Workshops), 2017 IEEE International Conference on.* IEEE, 308–313.

[4] Atmel. 2009. AVR Atmega 1284p 8-bit microcontroller. http://www.atmel.com/images/doc8059.pdf. (2009). [Online; accessed 13-April-2017].

[5] Atmel. 2014. AT86RF233 . http://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-8351-MCU_Wireless-AT86RF233_Datasheet.pdf. (2014). [Online; accessed 13-July-2017].

[6] G Avoine, MA Bingol, Ioana Boureanu, S Capkun, G Hancke, S Kardas, CH Kim, C Lauradoux, B Martin, J Munilla, et al. 2017. Security of Distance-Bounding: A Survey. *Comput. Surveys* (2017).

[7] Carsten Bormann, Mehmet Ersue, and A Keranen. 2014. *Terminology for constrained-node networks.* Technical Report.

[8] Stefan Brands and David Chaum. 1993. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques.* Springer, 344–359.

[9] Yvo Desmedt. 1988. Major security problems with the âĂŸunforgeableâĂŹ(Feige)-Fiat-Shamir proofs of identity and how to overcome them. In *Proceedings of SECURICOM*, Vol. 88. 15–17.

[10] Stefan Dziembowski, Tomasz Kazana, and Daniel Wichs. 2011. One-time computable self-erasing functions. In *Theory of Cryptography Conference.* Springer, 125–143.

[11] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti–jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing* 17, 4 (2014), 197–215.

[12] Ghassan O Karame and Wenting Li. 2015. Secure erasure and code update in legacy sensors. In *International Conference on Trust and Trustworthy Computing.* Springer, 283–299.

[13] metirionic. 2015. ATSAMR21-XPRO. http://www.metirionic.com/en/technology.html. (2015). [Online; accessed 13-July-2017].

[14] Job Noorman. 2017. Sancus: A Low-Cost Security Architecture for Distributed IoT Applications on a Shared Infrastructure. (2017).

[15] Daniele Perito and Gene Tsudik. 2010. Secure code update for embedded devices via proofs of secure erasure. In *European Symposium on Research in Computer Security.* Springer, 643–662.

[16] Alejandro Proano and Loukas Lazos. 2012. Packet-hiding methods for preventing selective jamming attacks. *IEEE Transactions on dependable and secure computing* 9, 1 (2012), 101–114.

[17] Dave Singelee and Bart Preneel. 2005. Location verification using secure distance bounding protocols. In *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on.* IEEE, 7–pp.

[18] Rodrigo Vieira Steiner and Emil Lupu. 2016. Attestation in Wireless Sensor Networks: A Survey. *ACM Computing Surveys (CSUR)* 49, 3 (2016), 51.

[19] Robert Wahbe, Steven Lucco, Thomas E Anderson, and Susan L Graham. 1993. Efficient software-based fault isolation. *ACM SIGOPS Operating Systems Review* 27, 5 (dec 1993), 203–216. https://doi.org/10.1145/173668.168635

[20] Nils Walravens. 2016. Operationalising the Concept of the Smart City as a Local Innovation Platform: The City of Things Lab in Antwerp, Belgium. In *International Conference on Smart Cities.* Springer, 128–136.

[21] Thomas Watteyne, M Palattella, and L Grieco. 2015. *Using ieee 802.15. 4e time-slotted channel hopping (TSCH) in the Internet of Things (IoT): Problem statement.* Technical Report.

[22] Fan Yang, Nelson Matthys, Rafael Bachiller, Sam Michiels, Wouter Joosen, and Danny Hughes. 2015. μ PnP: plug and play peripherals for the internet of things. In *Proceedings of the Tenth European Conference on Computer Systems.* ACM, 25.