

Flyweight RFID authentication with forward and backward security

Mike Burmester, Florida State University, Tallahassee,
Jorge Munilla, Universidad de Málaga, Spain

Abstract

The EPC Class1 Gen2 standard defines a platform for UHF RFID protocol interoperability, and supports basic reliability guarantees, provided by an on-chip 16-bit random or pseudo-random number generator (PRNG) and a 16-bit Cyclic Redundancy Code (CRC16). With such protection mechanisms conventional cryptographic security is particularly challenging. However we still face the security and privacy issues of the more powerful RFID systems.

Constrained devices are especially vulnerable to attacks that exhaust the range of their states. The only way to deal with such attacks is to regularly refresh the tags with high entropy randomness. Refreshing tags should make it hard to disambiguate earlier flows prior to refreshment given refreshed flows and conversely. This will guarantee forward and backward security.

We show that it is possible to secure identification by using only one pseudo-random number generator (PRNG) shared with the Server, and to provide forward security and backward security. We present an EPCGen2 compliant protocol that uses only three numbers drawn from a PRNG to authenticate tags when flows are not disrupted, and five numbers otherwise. In both cases there is synchrony, which guarantees availability.

We also have *session unlinkability* (weak anonymity), while the lookup time for the Server is constant. Furthermore we can extend this protocol so that at regular intervals the Server provides the tags with high entropy randomness. This can be done in a way that will support forward and backward security.

Finally, since no computations are involved during the authentication process (numbers are drawn in advance and stored locally), *online man-in-the-middle relay* attacks can be thwarted by having the Readers (but not the tags!) measure the time it takes for a response to a challenge to be received (Readers will need a timer to measure accurately time differences).

The implementation complexity for the PRNG is 1.5K logic gates, 190 clock cycles (at 100KHz), and 64B memory—so each 16-bit number is generated at 1.9ms (LAMED; the figures for the Self-Shrinking Generator are comparable).

References

- [1] BURMESTER, M., AND MUNILLA, J. A Flyweight RFID Authentication Protocol. In *RFIDSec09* (2009), The 5th Workshop on RFID Security, June 30 - July 2, Leuven, Belgium.
- [2] BURMESTER, M., AND DE MEDEIROS, B. The Security of EPC Gen2 Compliant RFID Protocols. In *ACNS* (2008), S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung, Eds., vol. 5037 of *Lecture Notes in Computer Science*, Springer, pp. 490–506.
- [3] BURMESTER, M., DE MEDEIROS, B., MUNILLA, J., AND PEINADO, A. Secure EPCGen2 compliant Radio Frequency Identification. In *ADHOC-NOW* (2009), P. M. Ruiz and J. J. Garcia-Luna-Aceves, Eds., vol. 5793 of *Lecture Notes in Computer Science*, Springer, pp. 227–240.
- [4] BURMESTER, M., VAN LE, T., DE MEDEIROS, B., AND TSUDIK, G. Universally composable RFID identification and authentication protocols. *ACM Trans. Inf. Syst. Secur.* 12, 4 (2009), 1–33.