On the (in)Security of Widely-used RFID Access Control Systems

Flavio Garcia
School of Computer Science
University of Birmingham

Abstract

Over the last few years much attention has been paid to the (in)security of the cryptographic mechanisms used in RFID fobs and contactless smart cards. Experience has shown that the secrecy of proprietary ciphers does not contribute to their cryptographic strength. Most notably the Mifare Classic, which has widespread application in public transport ticketing (e.g. Oyster) and access control systems, has been thoroughly broken in the last few years. Other prominent examples include KeeLoq and Hitag2 used in car keys and CryptoRF used in access control and payment systems.

This talk summarizes our own contribution to this field. We will briefly show some of the weaknesses we found in the Mifare Classic [dKHG08, GdKM+08, GvRVS09]. Then we will show that the security of its higher-end competitors like Atmel’s CryptoRF [GvRVWS10] and HID’s iClass [GdKGV11, GdKGV12, GdKGV14]–which were proposed as secure successors of the Mifare Classic–is not (significantly) higher. We will also cover security issues on vehicle immobilizers such as the Hitag2 key fob [VGB12] to conclude with a discussion on responsible disclosure principles.

References


