International Journal of Information Security, vol.24, no.3, pp.150-1-150-15, June, 2025.

Clonable key fobs: Analyzing and breaking RKE protocols

G. López López; R. Gesteira Miñarro; R. Palacios Hielscher

Abstract-

The automotive industry has been a target for cyber criminals for decades. New regulations have come into force in the automotive industry and manufacturers must take cybersecurity into account. One of the most interesting vehicle systems is the Remote Keyless Entry (RKE) system, which allows users to lock and unlock their cars, among other actions, with a remote control integrated in the car key. If this system is compromised, a malicious user could gain access to a vehicle remaining unnoticed. This paper presents the identification and analysis of a vulnerability in an RKE protocol that can be exploited to gain access to the car at any time, thus cloning the key fob. The reverse-engineering methodology used to uncover the vulnerability is outlined, along with other tested vehicles to show its applicability. A relevant aspect of the research is the fact that only open-source tools and available commercial hardware are needed to perform the analysis. This black-box approach is equally valid to learn RKE protocol features, without the need to extract and analyze ECU firmware, which is considerably more expensive. As a result, a detailed analysis of eight protocols from different manufacturers is shown and they are compared from a cybersecurity point of view, with one of them being totally broken.

Index Terms- Remote keyless entry; Radio frequency; Reverse engineering; Cybersecurity; Vehicle

Citation:
Gesteira-Miñarro, R.; López, G.; Palacios, R. "Clonable key fobs: Analyzing and breaking RKE protocols", International Journal of Information Security, vol.24, no.3, pp.150-1-150-15, June, 2025.