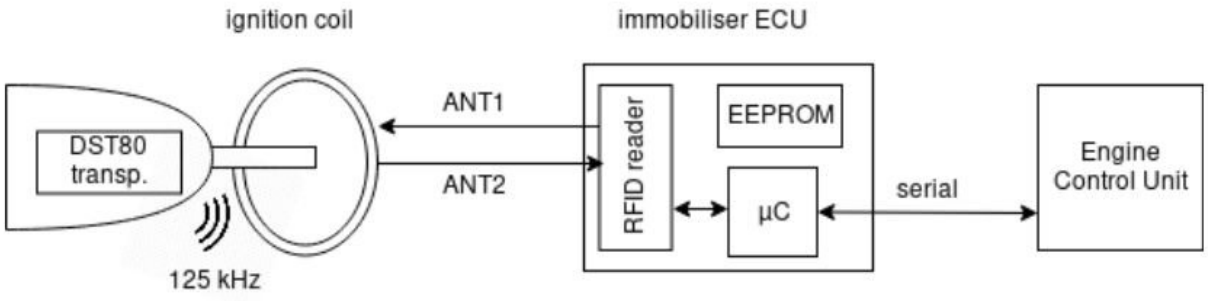
Insecure encryption configurations compromise security of Hyundai, Toyota, and Kia vehicles

March 7 2020, by Jelani Harper



A typical immobiliser system. Credit: Dismantling DST80-based Immobiliser Systems, DOI: 10.13154/tches.v2020.i2.99-127

Recent research indicates it's possible to infiltrate—and steal—vehicles manufactured by Toyota, Hyundai, and Kia due to flaws in the way their chip-enabled mechanical keys were encrypted.

According to a study published by KU Leuven in Belgium and the United Kingdom's University of Birmingham, an ineffective implementation of Texas Instruments' DST80 encryption allows potential hackers to clone the keys of these vehicles.

The research paper indicates the keys to this form of encryption are able to be discovered by reverse-engineering the firmware that supports them. Despite the fact that it's possible to leverage up to 80 bits of protection with DST80 encryption, certain Hyundai and Kia vehicles only use 24 bits—which can be rapidly bypassed in a matter of seconds on contemporary computers. Toyota vehicles affected by this vulnerability have encryption keys predicated on a serial number broadcast with the signal from their key fobs.

Because of how the DSTO encryption is built into the affected vehicles, intruders would simply need to get close enough to use Radio-Frequency Identification (RFID) scanners that can make the vehicles respond as though they were legitimate car keys. The data captured from even inexpensive versions of these devices is sufficient to figure out the encryption key for that particular vehicle it, copy it (with the same device), and use the device to disable part of the car's immobilizer.

Immobilizers are vehicle components that don't let cars start unless there's a proper key in the area. From there, intruders would only need to manipulate the key slot in the ignition barrel using well known techniques like starting them with screwdrivers or via hotwiring.

The research study publishes a full list of the models and years of the cars affected by this vulnerability. For the aforementioned manufacturers, the years span from 2009 to 2017 and include such popular models as Corollas, Land Cruisers, and Optimas. The study indicates that other vehicles not listed could be potentially affected by this issue as well.

The response from the automakers in question has been varied. Although a 2018 Tesla Model S is listed as one of the affected vehicles, the manufacturer issued an update in 2019 to redress this security issue. Toyota representatives commented that the vulnerability only applied to older vehicles because newer ones were configured differently. Hyundai representatives stated none of their affected vehicles are for sale domestically.

Vehicle owners with cars impacted by this vulnerability can protect them with manual methods like steering locks. As the Tesla example indicates, it is possible to reconfigure how the encryption is implemented to protect vehicles from this weakness.

More information: Dismantling DST80-based Immobiliser Systems, (PDF) doi.org/10.13154/tches.v2020.i2.99-127 , tches.iacr.org/index.php/TCHES/article/view/8546