

Millions of cars at risk of theft due to flaw in the development of keyless entry systems

August 15 2016



Credit: University of Birmingham

Researchers at the University of Birmingham have found that millions of cars could be vulnerable to theft, due to a flaw in keyless entry systems in many models.

The findings, presented at the 25th USENIX Security Symposium in Austin, Texas, highlight two case studies that outline the ease at which criminals could gain access to numerous vehicles with relatively simple and inexpensive methods.

Both attacks use a cheap, easily available piece of radio hardware to intercept signals from a key fob, and then employ those signals to clone the key.

Though most automotive immobiliser systems have been shown to be insecure in the last few years, the security of remote keyless entry systems (to lock and unlock a car) based on rolling codes has received less attention.

The team, from the School of Computer Science at the University of Birmingham, found that the security of the keyless entry systems of most VW Group vehicles manufactured between 1995 and today relies on a few, global master keys.

By recovering the cryptographic algorithms and keys from [electronic control units](#), a thief would be able to clone a VW Group [remote control](#) and gain unauthorised access to a wirelessly unlock practically every vehicle the Volkswagen group has sold for the last two decades, including makes like Audi and Skoda, by eavesdropping a single signal sent by the original remote.

A second case study outlines an attack that could affect millions more vehicles, including Alfa Romeo, Citroen, Fiat, Ford, Mitsubishi, Nissan, Opel/Vauxhall, Renault, and Peugeot.

The researchers devised a correlation-based attack on Hitag2, which allows recovery of the cryptographic key and thus cloning of the remote control with four to eight rolling codes and a few minutes of

computation on a laptop.

Dr David Oswald explained, "You only need to eavesdrop once. From that point on you can make a clone of the original remote control that locks and unlocks a [vehicle](#) as many times as you want. Manufacturers really need to take heed and review their security systems."

Dr Flavio Garcia added, "It's a bit worrying to see security techniques from the 1990s used in new vehicles. If we want to have secure, autonomous, interconnected vehicles, that has to change. Unfortunately the fix won't be easy, as there is quite a slow software development cycle, new designs will be quite a long time in the making."

The researchers suggest that car owners with affected vehicles avoid leaving any valuables in their car, and consider giving up on wireless key fobs altogether and open and lock their car doors the 'old-fashioned', mechanical way.

Provided by University of Birmingham

Citation: Millions of cars at risk of theft due to flaw in the development of keyless entry systems (2016, August 15) retrieved 4 May 2024 from <https://techxplore.com/news/2016-08-millions-cars-theft-due-flaw.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--