

Can an MP3 hack your car?

March 18 2011, by Katie Gatto



(PhysOrg.com) -- The idea that someone can get into your car without your permission isn't a new one. It's about as old as the coat hanger, but that was back in the days when you locks had a pull up button. We tend to think that digital car locks are safer, because it takes a higher level of sophistication to get into them, when Physorg [reported on it](#) in January, it was security professionals who were stealing the cars, but now it may be easier to boost your car, with the most innocuous of devices.

Researchers at the University of California, San Diego led by Stefan Savage, and Tadayoshi Kohno of the University of Washington, who have been looking at the vulnerabilities in electronic vehicle controls have found that cars that are built to be compatible with Bluetooth [wireless technology](#) have the potential to be hacked using that

connection.

The Bluetooth connection, which is designed to let your car and your phone work well together has the potential to be exploited in ways that would allow a less than scrupulous individual to upload [malicious code](#) to your car using an audio file. So, a song could literally give your car a virus. If you want to go one creepier, the researchers also found ways to pair the cars to a Bluetooth-enabled devices in order to execute that malicious code. So someone could be controlling your car, without you ever knowing it. The code can even be snuck in on an MP3. Burned onto a CD player, and put into your car. When the song is played becomes a [Trojan Horse](#) and can then alter the car's firmware, giving it access to the car's key systems.

The researchers would not comment on which model of car they had conducted this research on, only that it was a 2009 sedan with fewer [computer systems](#) than the average car, but we do know it was not a luxury car.

© 2010 PhysOrg.com

Citation: Can an MP3 hack your car? (2011, March 18) retrieved 10 April 2024 from <https://phys.org/news/2011-03-mp3-hack-car.html>

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.