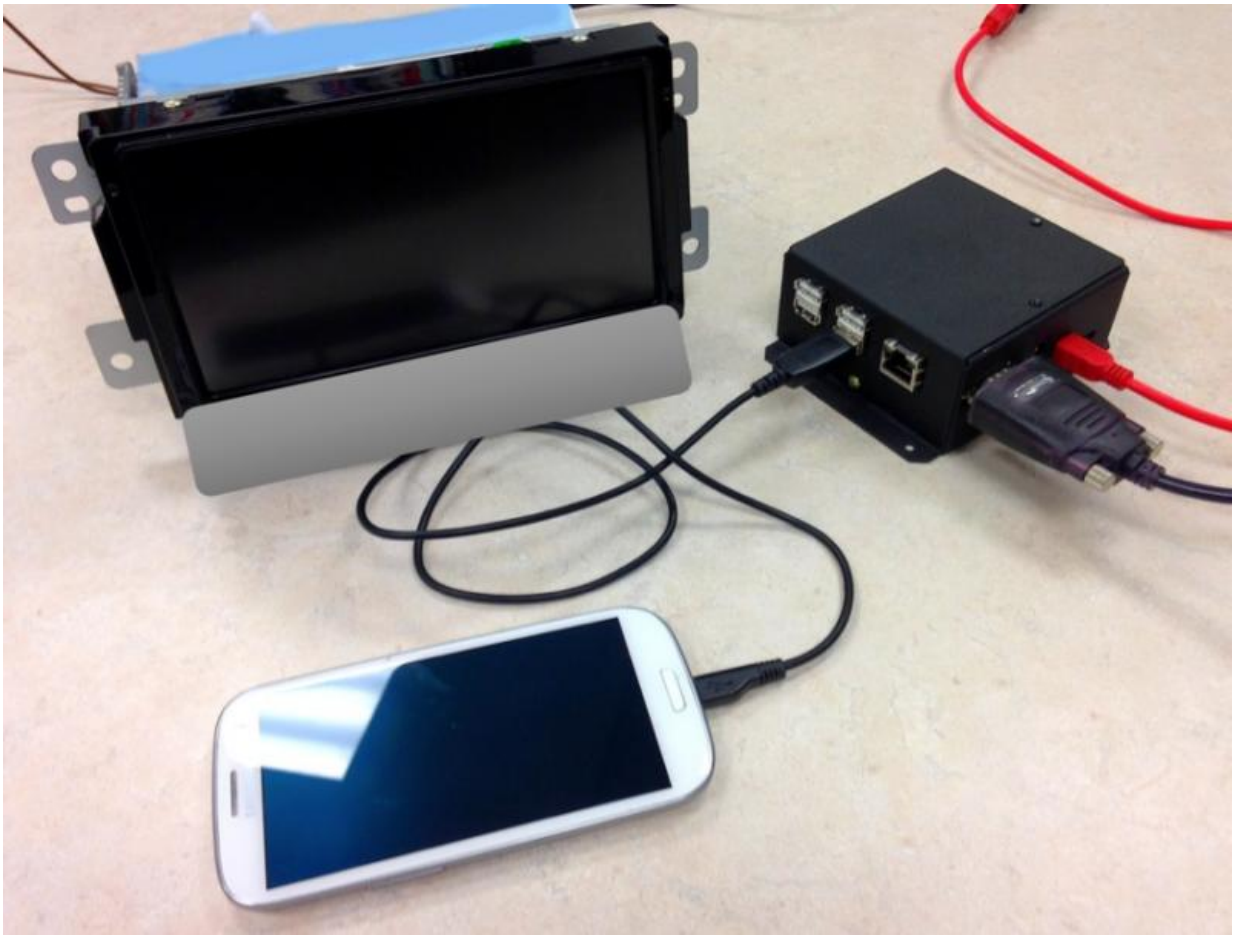
Researchers find vulnerabilities in cars connected to smartphones

September 1 2016



Credit: New York University

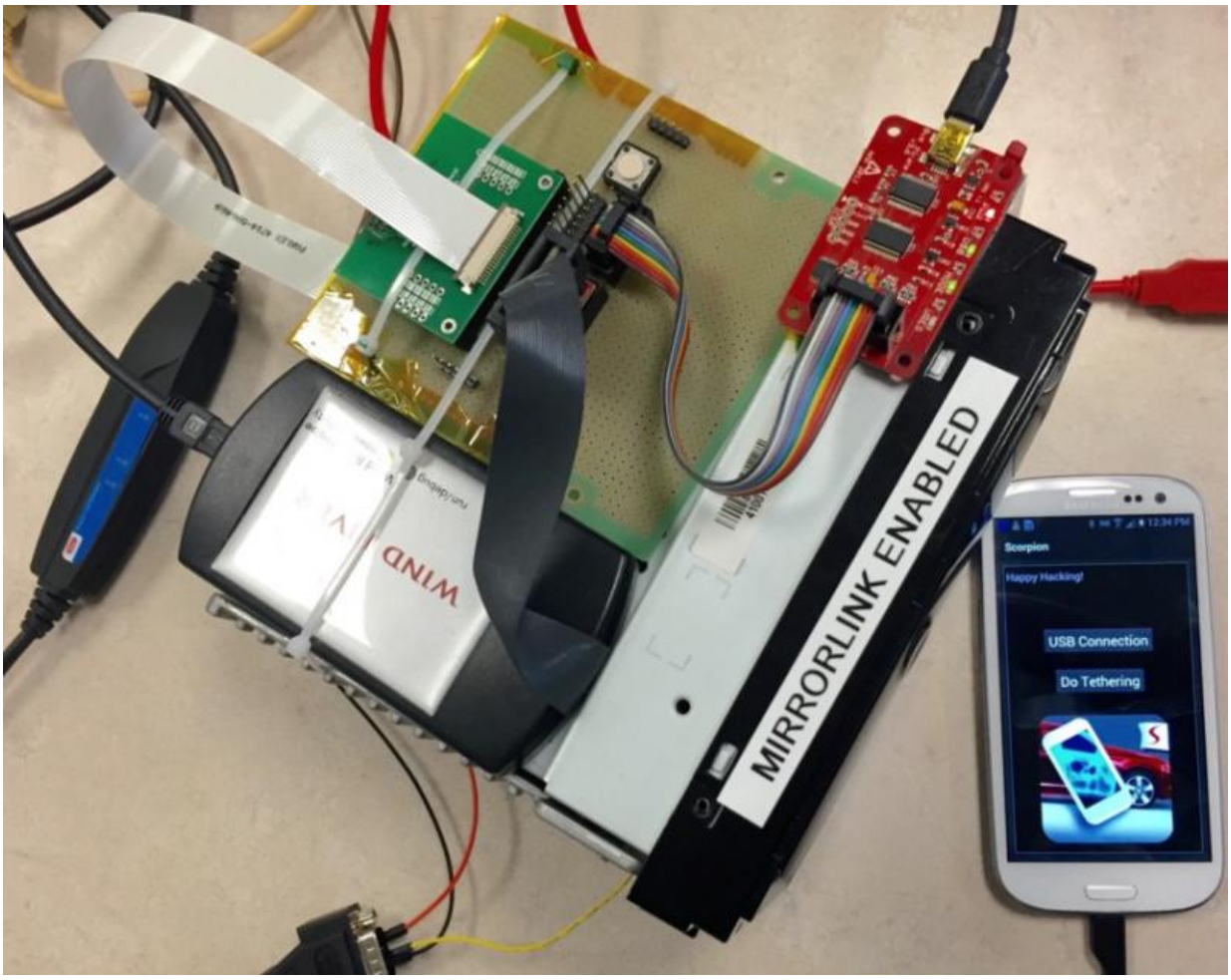
Many of today's automobiles leave the factory with secret passengers:

prototype software features that are disabled but that can be unlocked by clever drivers.

In what is believed to be the first comprehensive security analysis of its kind, Damon McCoy, an assistant professor of computer science and engineering at the NYU Tandon School of Engineering, and a group of students at George Mason University found vulnerabilities in MirrorLink, a system of rules that allow vehicles to communicate with smartphones.

MirrorLink, created by the Connected Car Consortium, which represents 80 percent of the world's automakers, is the first and leading industry standard for connecting smartphones to in-vehicle infotainment (IVI) systems. However, some automakers disable it because they chose a different smartphone-to-IVI standard, or because the version of MirrorLink in their vehicles is a prototype that can be activated later.

McCoy and his colleagues found that MirrorLink is relatively easy to enable, and when unlocked can allow hackers to use a linked smartphone as a stepping stone to control safety-critical components such as the vehicle's anti-lock braking system. McCoy explained that "tuners"—people or companies who customize automobiles—might unwittingly enable hackers by unlocking insecure features.



Credit: New York University

"Tuners will root around for these kinds of prototypes, and if these systems are easy to unlock they will do it," he said. "And there are publically available instructions describing how to unlock MirrorLink. Just one of several instructional videos on YouTube has gotten over 60,000 views." The researchers used such publically available instructions to unlock MirrorLink on the in-vehicle infotainment system in a 2015 vehicle they purchased from eBay for their experiments.

The automaker and supplier declined to release a security

patch—reflecting the fact that they never enabled MirrorLink. McCoy pointed out that this could leave drivers who enable MirrorLink out on a limb.

The authors hope their research, presented at the 10th USENIX Workshop on Offensive Technologies (WOOT '16) in Austin, Texas, will raise the issue of drivers unlocking potentially insecure features before IVI protocols such as MirrorLink are even more widely deployed.

More information: A Security Analysis of an In-Vehicle Infotainment and App Platform, by lead co-authors Sahar Mazloom and Mohammad Rezaeirad along with Aaron Hunter and McCoy, is available at www.usenix.org/conference/woot … presentation/mazloom

Provided by New York University