Don't connect your phone to rental cars

Christopher B. Hopkins | Friday, September 16, 2016

It is a great convenience to connect (or just charge) your smartphone when traveling in a rental car. But this convenience brings significant risks, as evidenced by a recent warning from the Federal Trade Commission (FTC) as well as a research paper from George Mason University. Users should know the risks, as well as preventative steps, and companies may want to consider implementing a "do not connect business phones to rental cars" policy.

On August 30, 2016, the FTC issued a warning to consumers entitled, "What is your phone telling your rental car?" FTC attorney Lisa Schifferle explained that automobile software often keeps "your mobile number, call and message logs, or even contacts and text messages." Some car systems may keep your GPS data, such as locations visited. If you are a frequent traveler, you have likely discovered this kind of residual data when you turned on the rental car (or paired your phone). While this scant information may initially seem harmless, such aggregated data could be used to develop identifying information about you or it may reveal confidential corporate information (e.g., contact names, text messages, phone numbers).

The FTC warning provides some guidance: avoid connecting your phone to rental car's system; charge the phone via the cigarette lighter port rather than directly from the car's USB port since it may silently access your data; and delete your data from the dashboard before returning your rental car. Specifically, check the car's system's setting menu to find the list of connected devices and make sure yours is deleted. If you downloaded an app to connect, make sure the app settings limit what is shared. The FTC warning, however, overlooks the fact that these risks also exist when leased vehicles are returned or vehicles are sold.

The research paper, "A Security Analysis of an In-Vehicle Infotainment and App Platform," revealed even greater concerns. Several car manufacturers have discontinued outdated proprietary dashboard systems for open, universal platforms which allow iPhones and Androids to seamlessly mirror the phone on the dashboard screen. An industry standard called MirrorLink certifies apps and devices. The researchers bought an infotainment system on eBay and hacked it to discover that MirrorLink's two security methods could be overcome since (a) bypassing information was already published online and (b) passwords were stored in unencrypted plaintext. The result was that hackers could "eavesdrop on and inject" malware into the vehicle's brain, the Controller Area Network, which could pose both a privacy risk as well as a personal safety risk.

Because more people are connecting their phones to cars, many of us are unknowingly transmitting personal information on our phones to rental cars where it can be accessed by future drivers. Worse, these infotainment systems, as they become more standardized, may not provide sufficient security, which is both a privacy and safety risk. Users should be careful pairing their phones with rental cars and, for leased or sold vehicles, take steps to delete data at the time of transfer.

Christopher B. Hopkins

Team member bio