Hacking Your Car â€“ What You Need to Know

July 23, 2015 â€“ Earlier this week, Wired Magazine released a story on hacking cars. Specifically, that hackers can gain access to virtually all of the systems available on new model cars. This is especially true for luxury vehicles because many of them now come standard with internet access. This really shouldnâ€™t have been a surprise to anyone - 60 Minutes released a similar story in February. But it does bring up some troubling questions. First, what are automobile manufacturers doing about this? And second, why in the world do the actual systems that operate a car need to be online at all?

View More: Previews News|60 Minutes News|Live News|More News Videos

Wiredâ€™s story focused on a vehicle manufactured by Chrysler. As with the video above, the team from Wired was able to gain access to all of the vehicleâ€™s operating systems.

Fortunately, in both of these cases, the hackers involved were â€œwhite hatâ€•. That means that they were doing good and turning over their results to the companies whose cars were at risk. Unfortunately, now that these hacks are known, it is probably only a matter of time before some teenage kid thinks it would be a lot of fun to scare his girlfriend by taking over the controls of her car.

The actual possibilities here are frightening if you start to think about them. A stalker could completely shut down his victimâ€™s vehicle on a lonely stretch of road. Or worse, a terrorist attack that shut down vehicles nationwide; snarling traffic and costing the country billions of dollars. One real possibility is that a hacker could take control of your vehicle and shut it down until you pay a ransom of several thousand dollars. Owners that donâ€™t pay could be prevented from ever using

their vehicle again. These are just a few of the possibilities.

Vehicle manufacturers are trying to release security patches for their software but thatâ€™s an uphill battle. Unless these patches are automatically downloaded and installed remotely, it is doubtful that most drivers will ever install them. And even if they are installed automatically, it may only take a day or two for hackers to find a work around. Manufacturers are likely to always be playing catch-up.

The manufactures will tell you that the reason the brakes on your car can be hacked and controlled via the internet is because all of the carâ€™s systems are tied into a single computer. And perhaps that is where the fix lies. It would be a fairly simple matter to add a second computer for the ignition, brakes and other automobile systems which isnâ€™t networked at allâ€¦ meaning absolutely no online access. Yes, it would add a cost to the vehicle, but it may be the only safe option.

Until then, automobile buyers need to know that they may be vulnerable to this type of attack. Until then, they may want to ask the manufacturer of their car to disconnect them from the internet entirely.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS