I Am The Cavalry

Assessment of BMW Door Lock Security Updates

There has been positive news in automotive cyber safety lately. BMW announced that they have fixed a flaw in over 2.2 million of their cars, silently and remotely. The flaw allowed someone other than the driver to remotely unlock the car, through the ConnectedDrive system. BMW pushed out an update over the mobile data network to the affected vehicles, and detailed further security measures they have taken to protect against accidents and adversaries.

The German Automobile Association (ADAC) investigated the cyber security of several BMW models and discovered six security flaws in the design and implementation of the ConnectedDrive software. They disclosed their research to BMW, who collaborated with ADAC researchers to understand and develop a fix for two of the most critical flaws. BMW remotely updated its customers' vehicles, adding HTTPS encryption and server authentication checks. BMW then announced the details of what they found, how they fixed it, and what other measures they have already taken to protect the safety of drivers, passengers, other vehicles, pedestrians, etc.

This is a big, positive step forward for cyber safety in automobiles. First, it shows that remote attacks against vehicles are still real threats, as demonstrated in 2010 and 2011 by security researchers. Second, this establishes the benefits of working with third-party technical experts, as well as the willingness of automobile manufacturers to engage security researchers acting in good faith. Third, it demonstrates the clear benefits of secure, remote update capabilities to shorten exposure time, reduce costs, and preserve customer confidence. Fourth, BMW gained credibility with customers and regulators by discussing the steps they have taken. Consequentially, taking cyber security seriously has given BMW a PR boost.

Despite these positive steps, some concerns remain. The problems ADAC researchers discovered – and that BMW subsequently fixed – have been solved for decades. It is concerning that the ConnectedDrive team either did not know about these potential issues or did not apply the fixes at that time. Newer vehicles were found to have better safeguards around ConnectedDrive, but the two improvements pushed out by BMW recently were not among these. The presence of these flaws to begin with, and the continued use of flawed software designs, also raises a question about the thoroughness and adequacy of internal processes and decision-making. Further, BMW did not say how critical car systems (such as braking, steering, and acceleration) are safeguarded from a compromise of the ConnectedDrive or other systems. Perhaps ADAC or other security researchers could investigate those potential issues in a similar way.

The following table is an overview of this story through the lens of I Am The Cavalry's Five-Star Automotive Cyber Safety Framework, released six months ago.

Framework	BMW Capability Demonstrated	
Safety by Design	No public attestation of Secure Development Lifecycle. No evidence of a sufficiently robust development process.	—
Third Party Collaboration	Clearly demonstrated their willingness to collaborate with third-party researchers acting in good faith.	★
Evidence Capture	No further information about these vehicles' ability to capture logs of system or network activity that could potentially expose further security gaps.	—
Security Updates	Clearly demonstrated their ability to update the ConnectedDrive system in a prompt and agile manner.	★
Segmentation and Isolation	No information provided on the physical or logical isolation measures separating critical systems (braking, steering, etc) from non-critical ones (door locks).	—

Note that information collected was not complete, so this rating likely does not represent BMW's full set of cyber safety capabilities.

In summary, BMW demonstrated capabilities aligned to two of the five stars in I Am The Cavalry's framework. These capabilities allow BMW to draw upon expertise and experience from those in the cyber security field, and facilitate continual improvement more quickly and inexpensively than other approaches. Issues still remain, but we are far ahead of where we were just a few years ago.

I Am The Cavalry is a global grassroots movement, formed in response to concerns over the impact of cyber security threats on public safety. We happily collaborate with others who share these goals, such as policy makers, government agencies, industry organizations, automobile manufacturers, public interest groups, and others. Our goal is not to supplant their judgment with ours, but to support and inform their decision-making to ensure safety.

For more information visit our website (https://iamthecavalry.org), or our Five-Star Automotive Cyber Safety Framework (https://iamthecavalry.org/auto/5star). Email us at info@iamthecavalry.org or on Twitter @iamthecavalry.

References

- http://www.autoblog.com/2015/02/03/bmws-connected-drive-feature-vulnerable-to-hackers/
- http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html
- http://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/sicherheitsluecken.aspx *(German)*
- http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/
- http://grahamcluley.com/2015/02/bmw-security-patch/
- http://www.autosec.org/publications.html
- https://www.iamthecavalry.org/domains/automotive/5star/
- https://www.press.bmwgroup.com/global/pressDetail.html?title=bmw-group-connecteddrive-increases-data-security-rapid-response-to-reports-from-the-german-automobile&id=T0202503EN
- http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf