BMW ConnectedDrive Vulnerability

AJ Trainor, Amalia Safer, Lily Houghton

Overview

- A German group of automobile security researchers found a vulnerability in BMWs
- Affected 2.2 million vehicles (including Rolls Royce and Mini models) manufactured after 2010
- Let the researchers unlock the cars without keys
- No cars appear to have been stolen through this vulnerability

ConnectedDrive

- Operates over cellular network
- Several smartphone apps can be used to unlock your BMWs

ADAC

- German automobile security research group
- Discovered a vulnerability
- Were able to “forge” the unlock-packet

Attack Process: Connecting to the BMW

1. Buy an IMSI Catcher and 3G/4G Jammer
2. Bring your new IMSI Catcher within range of a 2010 or newer BMW
3. Get the BMW to connect to you, by jamming the 3G/4G signals and exploiting 2G vulnerabilities

Exploiting ConnectedDrive

1. Using the IMSI Catcher, assign an IP to the vehicle*
2. Send the forged unlock packet over HTTP to the IP you chose
3. Open the door of your target BMW

* The IMSI catcher is simply the most straightforward way to obtain the IP of a phone/car within 40 feet of you.

Other Vulnerabilities

- BMWs manufactured before 2011 have a vulnerability in them that allow them to be started without keys:
- First, the attacker needs to get into the BMW
- Then they can use a “special device” to start the car, by copying identification details from the onboard diagnostic system

Immediate Fix

- Prevent arbitrary impersonation of the BMW server by using HTTPS with a valid certificate
- Have the unlock packet authenticated with, e.g., user identification and password details

How to be secure

- Hire security professionals
- Bug bounty programs
- Five Star Automotive Cyber Safety Program

FSACS

Five Star Automotive Cyber Safety Program:

- A standard for car manufacturing
- Includes useful tips about app updates, privacy, resilience testing, air gaps

The Moral

Anything that uses technology might not be secure. Do your research and maybe don't buy a BMW.

References

http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html
https://www.iamthecavalry.org/domains/automotive/5star/
http://www.tomsguide.com/us/hackers-unlock-bmws-remotely,news-20385.html
http://www.bbc.com/news/technology-31093065