OSTBAYERISCHE
TECHNISCHE HOCHSCHULE
REGENSBURG

Could a connected car be hacked?

Imagine jumping in your car but being taken somewhere you didn't want to go – driving the wrong way on a street, or even over a cliff. That may seem like an extreme scenario, but the danger is real. Hackers showed two years ago that they could remotely take control of a Chrysler Jeep.

As cars incorporate semi-autonomous features such as lane keeping, automatic distance control and self-parking, and their navigation and entertainment systems are connected to the internet, the amount of software code needed to control these systems is rising quickly. Keeping all these software programs updated has typically required drivers to visit the car repair shop.

Yet such repair-shop visits are a huge waste of time and money, so many automakers are introducing online software updates, also known as “over the air” or OTA updates. OTA updates give manufacturers the ability to respond quickly as problems come up. New features can be added, and bugs patched, in just an hour or two, all without troubling the car’s owner.

But there's no doubt that OTA updates also present a new set of risks. For a start, we've all, at one time or another, attempted to update the software on our computer or phone, only for the process to go wrong. An unusable car could be rather more of a problem than a "bricked" - or unusable - phone. In fact, in 2015, 15% of car recalls in the United States were related to software errors, up from 5% four years before.

Then there is the risk of "man-in-the-middle" attacks - hackers intercepting the updates before they reach the users. This is why OTA updates have to pass a number of security checks - Does the update have validation? Is it from a trusted source?

Manufacturers are also addressing the hacker threat by isolating the various systems in the car so that, for example, the radio is isolated from the steering wheel, and the engine from the brakes. Furthermore, each system protected by its own encryption.

Ultimately, as cars have become more connected, they become a bigger target for hackers. Carmakers know that consumer trust is critical, so security is the highest priority. The big question is whether the automakers are cleverer than the hackers.

Adapted from Woollacott, Emma (6 Oct 2017) “Could a hacker hijack your connected car?” BBC News. http://www.bbc.com/news/business-41367214 Date retrieved: 4 December 2017.

Task: *Answer the questions below **in English**. **Short answers** are acceptable for questions 1-7.*

1. What happened in the example with the Chrysler Jeep?

   It was hacked

2. Name three examples given in the text of modern software features in cars.

   a. Lane keeping

   b. Automatic distance control

   c. Self parking/Navigation systems/Entertainment systems

3. a. What do the letters "OTA" stand for?

   Over the air

   b. Briefly describe what an OTA update is.

   It is an online software uodate for cars/ OTA updates give manufacturers the ability to respond to problems as quickly as possible. New features can be added and bugs patched without the car owner needing to go to the car repair shop

4. a. What percent of car recalls were related to software errors in 2015? 15%

   b. What was the percent before? 5%

   c. When was this previous percent from? 2011

5. What is a "man-in-the-middle attack"?

   It is when hackers intercept the updates before they reach the users/destination.

6. What two types of security check are named?

   a. validation

   b. trusted source

7. How have carmakers adapted the software systems in cars to prevent hacking?

   a. they have isolated the systems e.g. radio from the steering wheel or the engine from the brakes

   b. Each system has its own encryption

8. Briefly summarize the advantages and disadvantages of OTA updates.

   Advantages – it is fast, easy for manufacturers and owners, fixes problems and patches bugs remotely. It can add new features. It can save time and money for the owner.

   Disadvantages – If it fails, the car may be unusable. It needs a reliable internet connection. Can be costly – both time and money - for the manufacturer. Security risks – hackers etc