Hackers not Crackers

Dear Reader,

In the USA, hackers recently accessed the CAN bus of a Jeep via the infotainment system and were able to control the car remotely. But were they crackers rather than hackers? The term "hacking" has fallen into disrepute and is now incorrectly equated with computer crime. But the criminals are actually crackers. They are the ones responsible for stealing online identities and exploiting weaknesses in systems. Crackers make malicious use of hackers' knowledge.

However, the two Jeep hackers, Charlie Miller and Chris Valasek, had good intentions. They were highlighting security vulnerabilities using a validated test process. Firstly, they changed the settings of the air conditioning and retuned the radio. Then they took control of the accelerator pedal and braked the vehicle while it was travelling at high speed. Despite taking manual countermeasures, the driver could not prevent or stop their interventions.

Professor Christof Paar, cryptography expert and holder of the Chair of Embedded Security at the Ruhr University Bochum, also has good intentions. "We must try to hack into systems with a degree of killer instinct. Drivers are not prepared for this sort of thing to happen and I think we urgently need to start carrying out penetration tests in the field." This means putting ourselves in the enemy's shoes. "It's a highly scientific process which is never-ending, because the attackers are constantly improving and adapting their methods," explains Paar.

Other experts are increasingly also warning of security vulnerabilities, in this case in the hardware. The industry is focusing too closely on software security. "For example, one important area of research is the design of hardware Trojans. This is all about finding out whether we can weaken systems by manipulating the hardware," says Paar. According to him this is a new approach, because in the past the emphasis has only been on finding and identifying manipulations.

For security experts this is a very unfortunate situation, because hardware, such as a CPU, can be manipulated at the very lowest level, either during the manufacturing process or even earlier during the design phase. "There are frighteningly few experts who know what this type of Trojan looks like," says Paar.

What does this mean for the engineers in the automotive industry? They could at least be given a so-called red team, whose members would look over their shoulders and show them how a cracker could attack and dismantle the system. Just like Miller and Valasek did. This is already happening to a limited extent, but the practice needs to be institutionalised.

With best regards

Markus Schöttle
Deputy Editor in Chief