Jeep Cherokee's Hacking and its Implications for Information Security

By Yashvendra Singh (http://bwcio.businessworld.in/author/yashvendra-singh/) on August 26, 2016

The debate about the sharing of responsibility between system security and information security continues, and it is still unclear, which of the two should be responsible for what type of intrusion.

By Dinesh Dholeh

The hacking of Fiat Chrysler's Jeep Cherokee set off a flurry of activity in the automobile security space, and everyone was quick to point fingers at the infotainment system that was the source of the intrusion. With as many as 1.4 million cars recalled, the cost of this successful intrusion was pretty high, to say the least.

The standards for safety and security, however, are empirically divided. We have functional safety standards in ISO 26262 and information security standards in ISO 27001:2013. In the Cherokee incident, the infotainment system and the vehicle's braking systems met standards but were deemed not "non-

compliant" because of the intrusion. The other areas of vulnerability identified were the onboard diagnostic (OBD) ports and over-the-air (OTA) updates.

So where was the problem? It was finally concluded that the vulnerability was with respect to adherence to the data security standards as governed by ISO 27001:2013 instead of an infotainment weakness. However, the situation is that the infotainment system was hacked and the vehicle's control systems were handed to the hacker on a platter.

Whether the non-conformance was for ISO 26262 or ISO 27001:2013, the important part is what was eventually compromised. It was the safety of the driver, passengers, and potentially other motorists on the road that would have been ultimately affected by the intrusion.

The investigation revealed that infotainment systems with open ports are not mature enough to reject commands from unauthenticated sources and hence vulnerable to intrusions. In an earlier era, hackers could send rogue voltages and damage printers that were connected to the victim. Today, printers and other devices that are connected to the computer have circuitry that prevents damage caused by rogue currents coming from the wrong source.

This is rather similar to how hackers used the ability of the infotainment port to "listen and accept commands." The question that end-users would like to ask is this: just like modern computer printers and peripherals, shouldn't we also secure critical processes of an automobile from rogue commands being executed out of the ordinary? Whether done genuinely or maliciously, when the possibility of the commands resulting in a hazard is high, the need for security against intrusion is paramount.

However, an OEM needs to be able to ask simple questions such as for the brakes:

o Should the system allow the brakes to be disabled when the engine is on?

o Even more so, should the brakes be allowed to be disabled when the automobile is in motion?

o Most so, should the brakes be allowed to be disabled at all?

For the throttle, the questions are:

o Should throttle control be allowed by any other device but the gas pedal?

o Even if it were allowed, shouldn't it take permission from the driver, such as with a voice or code activated command from the driver?

o Even so, should there not be a feature to override this from behind the steering wheel?

o Should all critical commands be encrypted?

Compromising the safety of the passengers and motorists in the immediate surroundings is not something that automotive manufacturers, or for that matter, regulators, can pass off as a standoff on standards. Whether it was a nonconformance with respect to ISO 27001 or ISO 26262, the result was a potential hazard. Fortunately, this event unfolded under controlled circumstances as opposed to any actual exploitation of such vulnerabilities, which will be anything but controlled.

The debate about the sharing of responsibility between system security and information security continues, and it is still unclear, which of the two should be responsible for what type of intrusion. The road ahead is, however, very clear: there will be an increasing sharing of risk and responsibility of intrusion prevention. From an end-objective perspective, there will be either an overlap or convergence in ISO 26262 and 27001 conformance requirements.

In the future, instruments and automobile systems will require self-validation of commands. To achieve this, they would require a certain degree of analytical ability programmed into them, to help differentiate a malicious command from a genuine one.

QuEST Global's automotive team is working with some Tier 1 vendors and OEMs to help them to address and solve some of these challenges and ensure fool-proof conformance to all safety standards meeting the needs of the automobile industry of the future.

(The author is Strategic Initiatives Leader, Automotive, QuEST Global)