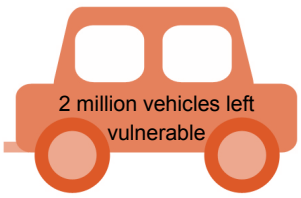
QONEX
THE CONSULTING ARM OF NEXOR

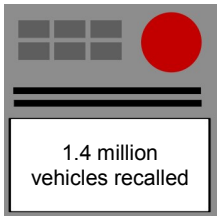
Best Research Poster
2015 IAAC Symposium

IMPROVING CYBER SECURITY IN THE AUTOMOTIVE SECTOR



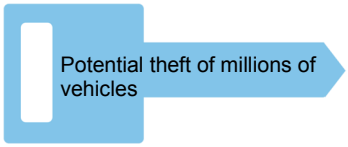
February 2015 – Cyber security hole via key fob leaves more than two million BMWs vulnerable.

(Source: Autoblog)



July 2015 - Chrysler issues a recall notice to fix its infotainment system software.

(Source: Computer World)



July 2015 – Court order stops publication of codes used to start luxury cars.

(Source: Guardian)

August 2015 - Hackers disable Corvette brakes by texting insurance dongle.

(Source: International Business Times)

WHY ARE THESE ISSUES ARISING?

The automotive industry is built around best practice for hardware engineering. Overlying this with software engineering and cyber security principles is complex.

The amount of software code in cars is increasing rapidly with high-end cars often having more than 100 million lines of code.

The automotive industry is pushing ahead rapidly with innovation, which will only increase the volume of software.

The longevity of vehicles (10-15 years) challenges traditional approaches to keeping software up to date.

"A clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who may wish to collect and use personal driver information."

(Source: US Senator Edward Markey report)

THE NEED TO DO BETTER

If the software of automotive companies fails, then customers could be put at risk and the companies could;

- be prosecuted under product liability laws;
- be prosecuted under health and safety laws;
- suffer severe reputational damage;
- be fined up to 2% of global turnover under the EU's General Data Protection Regulation.

"It is 30 times more expensive to fix a vulnerability during post-production than during the design, requirement identification and architecture stage."

(Source: National Institute of Standards & Technology - NIST)

HOW TO TACKLE THE PROBLEM?

Security is more than just applying patches. It is about robust architectures that isolate subsystems, and about systems that detect and react to abnormalities, something traditional vehicles have not had to deal with.

One element of the solution is ensuring software is trustworthy by following standards such as PAS 754. Sponsored by the Trustworthy Software Initiative, PAS 754 can be integrated with ISO 26262, the automotive safety standard, via TickITplus.

"A document such as PAS 754 is important because it can help to close down the trapdoors in an organisation's software platform that leave it vulnerable to cyber attack."

(Howard Kerr, Chief Executive of BSI)

+44 (0)115 952 0500 info@qonex.com www.qonex.com

P-0057-1015