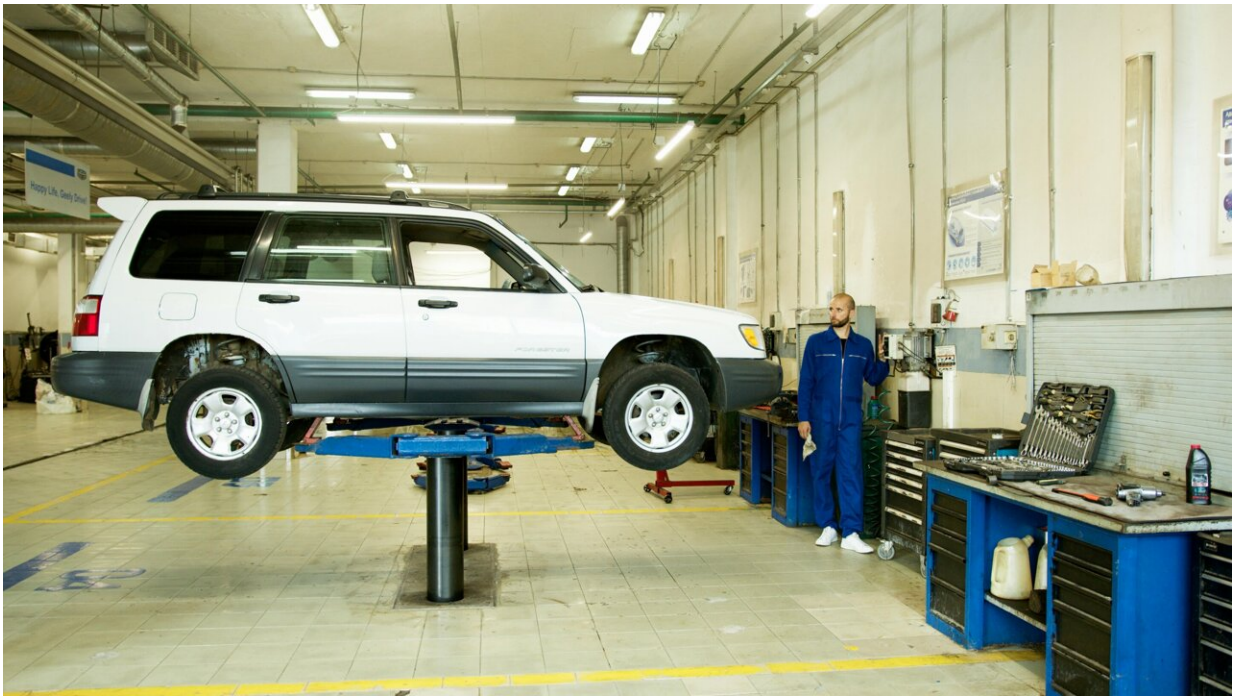
Scientists find major gaps in cybersecurity at auto workshops

May 28 2024, by Christian Boström



Credit: Artem Podrez from Pexels

In a new study from the University of Skövde, researchers found that many auto workshops do not know enough about how to keep our cars safe from cyberattacks. "A large proportion of the vehicle fleet could practically be entirely open to attacks or already breached," says Marcus Nohlberg, docent in cybersecurity at the University of Skövde.

Modern cars can be described as connected advanced computers on wheels, and these computers handle everything from anti-skid systems to adaptive cruise control.

Recently, car computer systems have also started communicating with each other. This communication occurs outside the car. The intention is to avoid collisions, but it also opens up risks, and cars can become targets for cyberattacks. In 2015, two security researchers demonstrated how they could take control of a Jeep Cherokee's brakes and steering.

However, the new study from the University of Skövde, published in *Information & Computer Security*, shows that security awareness and knowledge among auto workshops are still low when it comes to cybersecurity. So, what happens if auto workshops do not have the necessary knowledge or awareness to handle car software correctly?

"A large proportion of the vehicle fleet could practically be entirely accessible to attacks or already breached," says Nohlberg, who, together with Martin Lundgren, senior lecturer in informatics, and David Hedberg, a former student at the University of Skövde, is behind the study.

But the extent is difficult to assess. This is due to a lack of transparency in how car manufacturers operate. One issue highlighted in the study is that car manufacturers have devised a solution for managing software exclusively accessible to authorized workshops. This exclusivity fosters significant uncertainty regarding the proper handling of the software, consequently leading to unaddressed security concerns.

"This is particularly true for workshops that are not authorized. They are often forced to use unofficial methods to manage the cars. For most people, the car is the most advanced computer they have, but they currently have no way to influence updates and information security,"

says Lundgren.

The researchers behind the study believe that both the public and professionals need greater insight into the systems. If more than just authorized workshops were allowed to use official software to update cars and had insight into the car's security, it would benefit safety. The current situation makes sense from the manufacturers' perspective, but the consequences for owners and society at large could be enormous.

"A large portion of the vehicle fleet may have significant vulnerabilities without us having any opportunity to control or protect ourselves against them at all. For us, it has been an eye-opener that there are such significant previously unknown risks in the automotive industry that are not being addressed," says Nohlberg.

More information: David Hedberg et al, Cybersecurity in modern cars: awareness and readiness of auto workshops, *Information & Computer Security* (2024). DOI: 10.1108/ICS-11-2023-0211

Provided by Swedish Research Council