Autonomous Vehicles and Cybersecurity:

Risks, Realities, and the Case for Transparency

Carl Lochstampfor Jr

Department of Cybersecurity, Old Dominion University,

CS 462 — Cybersecurity Fundamentals

February 13, 2026

Answer both of the following questions:

1. What are the implications of vehicle hacking for autonomous vehicles? Today's vehicles have complex computer code and autonomous vehicles will have even more complex code. Do you think we will ever have widespread use of safe autonomous vehicles? Why or why not?
2. One of the suggestions to improve vehicle security is for car manufacturers to release their code open source to allow for public scrutiny. Do you think this would help improve vehicle security? Why or why not?

Article Chosen

- "CONNECTED CARS: Is your internet-enabled vehicle safe from hackers?", IOL.CO.ZA, Jun 30, 2021, https://www.iol.co.za/motoring/industry-news/connected-cars-is-your-internet-enabled-vehicle-safe-from-hackers-af650f21-d7ec-49ef-8c97-c1cb605f947dLinks to an external site.

Autonomous Vehicles and Cybersecurity: Risks, Realities, and the Case for Transparency

Question 1

Vehicle hacking is a serious concern for autonomous vehicles since modern cars already rely heavily on software, and adding autonomy will make them even more complex. The IOL article points out that connected vehicles gather and share a lot of data, including driving habits and personal account details (Ruthun, 2021). The biggest risk is not just data theft, but the possibility of someone taking physical control of the vehicle.

The 2015 Jeep Cherokee hack showed that attackers could control steering and braking from a distance. Miller and Valasek found a flaw that put 1.4 million vehicles at risk, proving remote attacks are possible (Erwin, 2021). If today's cars can be hacked, fully autonomous vehicles, which rely completely on software for steering, acceleration, and braking, could be even more vulnerable.

Even with these risks, I think it is possible to have safe autonomous vehicles on a large scale, but it will take time. The benefits, such as vehicle-to-vehicle communication, better traffic flow, and improved safety, are too important to overlook (Ruthun, 2021). Still, making progress will require:

- Industry-wide cybersecurity standards
- Stronger regulatory oversight (e.g., NHTSA involvement)
- Security-first engineering practices

Question 2

Just as seatbelts and airbags became standard over many years, automotive cybersecurity will improve as regulations, public demand, and technology advance. Like seatbelts and airbags, which became standard over many years, automotive cybersecurity will improve as regulations, public demand, and technology advance. Ode to open source could improve security—but only with a structured implementation.

The Jeep vulnerability went unnoticed for years until ethical hackers found it. Open-source ideas suggest that more people looking at the code makes it more likely that problems will be found sooner. Being transparent helps keep companies accountable and lets independent security experts check the code before attackers can take advantage of it.

Some people say that sharing source code gives hackers a guide. However, the Jeep case shows that hiding code does not prevent determined attackers from understanding how systems work (Erwin, 2021). Security should be based on strong design, not on keeping things secret.

A mixed approach is the most practical. Safety-critical systems could be reviewed openly or checked by third parties, while companies can still protect their unique features. Working together openly, along with strict certification and compliance rules, would probably make automotive cybersecurity stronger, not weaker.

References

Erwin, B. (2021, February 25). *The groundbreaking 2015 Jeep hack changed automotive cybersecurity*. Fractional CISO. https://fractionalciso.com/the-groundbreaking-2015-jeep-hack-changed-automotive-cybersecurity/

Ruthun, P. (2021, June 30). Connected cars: Is your internet-enabled vehicle safe from hackers? *IOL*. https://www.iol.co.za/motoring/industry-news/connected-cars-is-your-internet-enabled-vehicle-safe-from-hackers-af650f21-d7ec-49ef-8c97-c1cb605f947d