How do drivers respond to vehicle cyberattacks? A driving simulator study

Jah'inaya Parker[1], Fangda Zhang[2], Meng Wang[1], Shannon C. Roberts[1]
[1]University of Massachusetts, Amherst, MA, USA
[2]The Abigail Wexner Research Institute at Nationwide Children's Hospital, Columbus, OH, USA

Modern vehicles are embedded with numerous electronic components, making them more advanced and automated, while also making them vulnerable to cyberattacks. This study investigated how drivers respond to unexpected, cyber-attack-induced situations through a driving simulator study. It also examined differences in driver responses if they were trained or received warning messages on how to mitigate the effect of a vehicle cyberattack. The findings suggest that drivers' responses to cyberattacks vary based on the severity of the event. Those who receive training are much more likely to drive cautiously when the vehicle behaves unexpectedly and those who receive warning messages are likely to view them, but not necessarily take action. These results have far reaching implications into the utility of training programs in improving driver behavior and leave future work in terms of optimizing warning message systems.

INTRODUCTION

Due to drivers' increasing demand for in-vehicle entertainment options and the rapid development of technologies, modern automobiles are more than mechanical machines used for transportation (Eiza & Ni, 2017; Zhang, Petit, & Roberts, 2019). Vehicles are embedded with numerous electronic components, making them more advanced and automated, and allowing the possibility of internal and external vehicle connections. While intended to facilitate driving, the evolution also brings up cybersecurity issues: modern vehicles are vulnerable to cyberattacks.

Hackers can propagate cyberattacks on vehicles through several avenues, including physical and remote access (Hodge, Hauck, Gupta, & Bennett, 2019). A Jeep Cherokee was hacked by two researchers remotely from their basement and a Mitsubishi Outlander was hacked through manipulations between its mobile app and the Wi-Fi access point (Eiza & Ni, 2017; Zhang et al., 2019). Moreover, almost 100 million Volkswagen vehicles manufactured between 1995 and 2016 were vulnerable to remote, keyless-entry hacks (Garcia, Oswald, Kasper, & Pavlidès, 2016; Zhang et al., 2019).

The increasing number of electronic components, external connections, and communications embedded in vehicles account for their vulnerability to cyberattacks (Larson & Nilsson, 2008). Research has begun to address the issue by theoretically analyzing the attack surface and listing the potential outcomes. As a consequence, general recommendations regarding system design have been proposed to prevent future vehicles from cyberattacks. However, a prominent feature of cyberattacks is their randomness and unpredictability (Petit & Shladover, 2014). Combined with how fast technologies evolve and vehicle systems update, there is no panacea to prevent all vehicle cyberattacks (Zhang et al., 2019). Additionally, it is believed that the majority of software and hardware systems in vehicles are not protected against manipulations and that existing automotive systems tend to be fragile (Koscher et al., 2010; Wolf, Weimerskirch, & Wollinger, 2007; Zhang et al., 2019).

Because drivers are those who directly interact with vehicles and would respond to any potential cyberattacks, it is critical to consider their role and investigate their response behavior under such situations. Doing so would allow us to assess the consequences of vehicle cyberattacks in terms of driver safety (Cranor, 2008; Zhang et al., 2019). Yet, past research has not thoroughly studied the drivers' behavior in the context of vehicle cyberattacks.

While there is no one-size-fits-all solution to prevent vehicle cyberattacks, training and warning systems are effective in helping drivers deal with unexpected and hazardous situations (Zhang et al., 2019). Therefore, we hypothesized that if drivers could be trained on vehicle cybersecurity and receive warning messages when encountering vehicle cyberattacks, they may safely respond to cyberattack-inducted situations. Regarding drivers' response in safety-critical situations, various measures such as their glance behavior toward the side mirrors or the rear mirror, pulling the car over, and using information from inside of the vehicle for assistance are indicators as to whether the situation is properly and safely handled (Classen et al., 2010).

The present study examined how drivers respond to vehicle cyberattacks through a driving simulator study. A secondary goal was to investigate how training and warning systems affect drivers' response behavior toward such attacks. By doing so, we aimed to quantify and characterize drivers' behavior under such safety-critical situations and eventually, offer insights into vehicle cybersecurity from the perspective of drivers themselves as well as possible solutions that consider both the drivers and vehicle systems.

METHODS

Phase I of this project focused on the iterative development of the training and warning systems using the human centered design process. Phase II evaluated the effectiveness of the training and warning systems in a driving simulator study and is described below.

Participants

A total of 32 participants (aged 18-26; 23 males, 7 females, and 2 non-conforming individuals) were recruited from a university campus and the surrounding town using flyers and email advertisements. A power analysis showed that with a sample size of 32 and an effect size 0.38, when setting the alpha error to 0.05, the power is 0.8. The average age of

the participants was 20.4 years (SD = 2.0 years). Only individuals with a valid United States driving license were included in the study. Participants were randomly split into four groups: training only, warnings only, training + warnings, and no intervention (control group).

Simulation Environment and Equipment

A fixed-based RTI (Realtime Technologies Inc.) driving simulator consisting of a fully equipped 2013 Ford Fusion surrounded by six screens with a 330-degree field of view was used for the study (Figure 1). The cab has two dynamic side-mirrors, providing participants with realistic side and rear views of the scenarios. In the car, there is a fully customizable virtual dashboard and center stack.

Figure 1: RTI driving simulator

During each drive, participants were recorded using the video capture and review system, Sim Observer. Two cameras recorded the participant's hand and foot movements, as well as the forward view and dashboard (Figure 2).

Figure 2: Camera view of hand and foot movements along with forward roadway and dashboard

Driving Environment and Scenarios

The driving environment consisted of long sections of roadway with four straight sections and four curves – a loop – with no traffic lights or stop signs, and a speed limit of 35 (Figure 3). Drivers experienced a total of four scenarios/drives: the first was a baseline drive whereas the next three drives contained cybersecurity events. All cybersecurity events occurred when the driver was entering the last straight section. Table 1 lists and describes the three cybersecurity events in the order they were presented to participants. The cybersecurity events were chosen based on past literature (McCarthy, Harnett, & Carter, 2014).

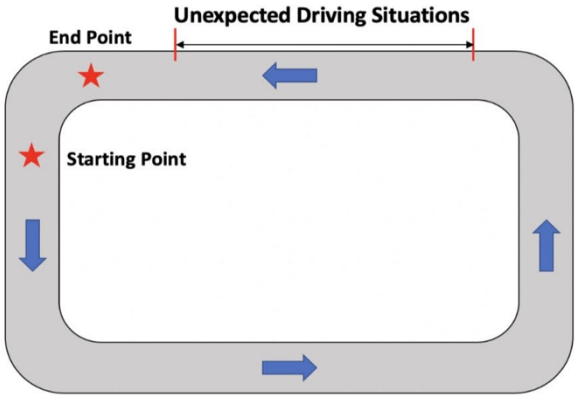


Figure 3: Layout of driving scenario

Training and Warning System

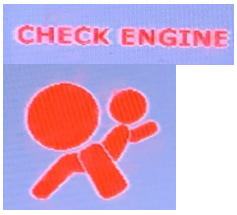
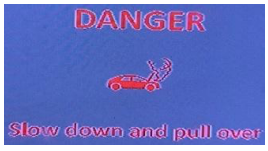
Participants in the training and training + warning group received training before being exposed to the cybersecurity events (i.e., between the first two drives). This training informed participants of the dangers of vehicle cyberattacks and how to respond to cyberattacks. Participants were tested on their knowledge using scenes (e.g., "What would you do if your vehicle changed lanes by itself?"). Participants in the warning and training + warning group had in-vehicle warning messages appear, as shown in Table 1. The warning was dependent on the severity of the cybersecurity event and was issued approximately 5 seconds after the cybersecurity event began. The warnings were designed and developed based on the feedback that we received from our previous user-centered design experiments as well as general guideline for warning design (Baldwin & Lewis, 2014; Wogalter & Mayhorn, 2005).

Driving Measures and Dependent Variables

To ascertain which behaviors were indicative of a driver responding to a cyberattack, the research team viewed and annotated a portion of the videos. For example, looking in the rearview mirror for an emergency vehicle during the Siren scenario or exhibiting large steering wheel movements when trying to gain control during the Lane Change scenario were both expected reactions. A total of 11 behaviors (i.e., dependent variables) were included in the analysis: hand hesitation, foot hesitation, changing the number of hands on wheel, checking the side mirror, checking the rearview mirror, looking at the dashboard for airbag or check engine message, looking at the dashboard for a warning message, large steering wheel movement, changing lanes, pulling over, and slamming the brakes. For the 11 dependent variables, the Spearman's correlation coefficient was evaluated, and all pairs were not found to be correlated except for the "hand hesitation" and "changing number of hands on wheel" ($\rho = 0.22$, $p = 0.03$).

Participants' responses were determined from the videos recorded in Sim Observer. Coding started from the moment the cybersecurity event began. For each video, a researcher noted the time when the participant did one of the 11 predetermined reactions. To ensure accuracy and reliability, three researchers coded the videos for the same two participants and any discrepancies were rectified.

Table 1: Cybersecurity Event Descriptions and the Associated Warning Message

Event Type	Warning Message
Sirens Sirens, similar to a police car or ambulance, begin to play.	Audio states "Your comfort and convenience might be impacted. Distraction might be caused". Image appears on the dashboard. 
Dashboard Signs A single high-pitched beep sounds and the two warning signs illuminate on the dashboard. 	Audio states "Your comfort and convenience might be impacted. Distraction might be caused". Image appears on the dashboard. 
Lane Change The vehicle is suddenly controlled by the experimenter, who repeatedly moves the vehicle from the left lane to the right.	Audio states "Your safety is compromised. Slow down and prepare to pull over". Image appears on the dashboard. 

Data Analysis and Independent Variables

For all dependent variables, the equality of the mean and variance was examined to determine the appropriate model: either Poisson or logistic regression. Six variables were best suited for Poisson regression, including the count of: hand hesitation, foot hesitation, changing number of hands on wheel, changing lanes, looking at dashboard for airbag or check engine messages, and slamming on brakes. The other 5 variables were modeled using logistic regression where the counts were converted to a binary format: 0 – if the behavior never occurred or 1 – if the behavior ever occurred.

With both Poisson and logistic regression models, there were two independent variables: group (control, training, warning, and training + warning) and drive (Sirens, Dashboard Signs, and Lane Change). As these were both categorical variables, we selected a reference level of control for the group variable and Dashboard Signs for the drive variable.

RESULTS

Table 2 indicates the average number of times each participant engaged in each of the activities per drive (for the first 6 activities that were modeled using Poisson regression). For the last activity that was modeled using logistic regression, Table 3Table 2 indicates the percentage of participants who engaged in the activity for the lane change drive. No large steering wheel movements were recorded for the Siren or Dashboard Signs drives.

Table 2: Average number of times each participant engaged in the activity per drive for six of the dependent variables

Variable	Group	Drive		
		Siren	Dashboard Signs	Lane Change
Hand hesitation	Control	0.000	0.000	0.375
	Training	0.000	0.000	0.125
	Warning	0.000	0.125	0.000
	Training + Warning	0.000	0.000	0.250
Foot hesitation	Control	0.375	0.250	0.375
	Training	0.250	0.250	0.250
	Warning	0.125	0.250	0.750
	Training + Warning	0.143	0.125	0.125
Change hands on wheel	Control	0.375	0.625	0.625
	Training	0.375	0.125	0.250
	Warning	0.000	0.375	1.250
	Training + Warning	0.286	0.375	0.375
Change lanes	Control	0.250	0.500	0.125
	Training	0.125	0.250	0.375
	Warning	1.000	0.375	0.000
	Training + Warning	0.000	0.125	0.250
Look at dash for airbag or engine messages	Control	0.000	0.000	0.000
	Training	0.000	0.000	0.000
	Warning	0.625	2.625	1.500
	Training + Warning	0.571	1.125	0.750
Slam on brakes	Control	0.000	0.000	0.000
	Training	0.000	0.000	0.125
	Warning	0.000	0.000	0.250
	Training + Warning	0.000	0.000	0.125

Poisson regression and logistic regression models were applied on each response variable. Among the dependent variables, hand hesitation, foot hesitation, changing number of hands on wheel, changing lanes, looking at dashboard for airbag or check engine messages, slamming on brakes, and large steering wheel movement were not statistically significantly associated with the independent variables and/or had a poor model fit (using the Pearson's Chi-Square statistic).

We present the findings from the statistical analysis for the remaining four variables that had good model fit (look at dashboard to check for warning messages, check rearview mirror, check side mirror, and pull over) in the proceeding

sections. These four significant dependent variables were all modeled using logistic regression and we present the percentage of participants who engaged in a certain activity.

Table 3: Proportion of participants who engaged in large steering wheel movements during the lane change drive

Group	Proportion
Control	0.875
Training	0.625
Warning	1.000
Training + Warning	0.625

Look at dashboard to check for warning messages

Figure 4 summarizes results for looking at the dashboard to check for warning messages. The group factor was significant: the warning group, versus the training + warning group, decreases the log odds of looking at the dashboard by 1.42 ($\beta = 1.42$, $SE = 0.71$, z-score = -2, $p < 0.05$). The goodness of fit test was not significant ($p = 0.1$), implying that the model fit the data.

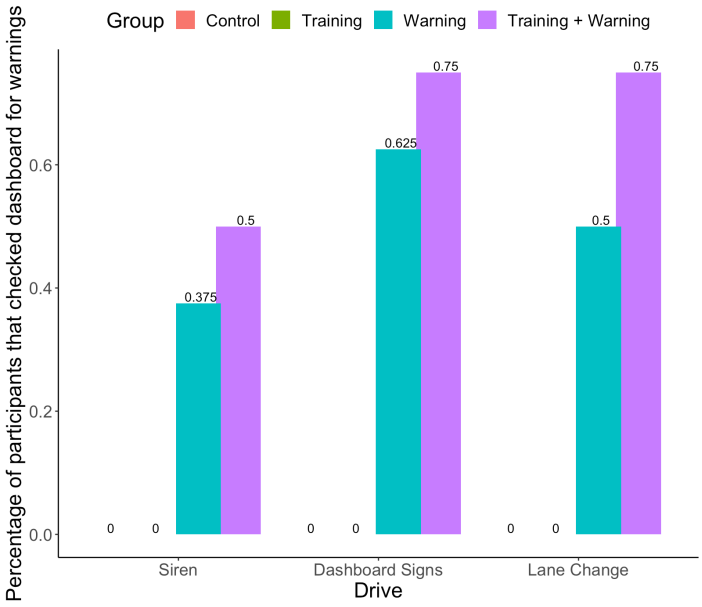


Figure 4: Percentage of participants who checked the dashboard for warning messages, separated by group

Check rearview mirror

Figure 5 summarizes results for checking the rearview mirror. The siren factor was significant: the Sirens scenario, when compared to the Dashboard Signs scenario, increases the log odds of checking the side mirror by 3.22 ($\beta = 3.22$, $SE = 0.82$, z-score = 3.92, $p < 0.01$). The goodness of fit test was not significant ($p = 0.3$), implying that the model fit the data.

Check side mirror

Figure 6 summarizes results for checking the side mirror. The lane change factor was significant: the Lane Change scenario, relative to the Dashboard Signs scenario, decreases the log odds of checking the side mirror by 1.4 ($\beta = 1.4$, $SE = 0.68$, z-score = -2.06, $p = 0.04$). The goodness of fit test was not significant ($p = 0.76$), implying that the model fit the data.

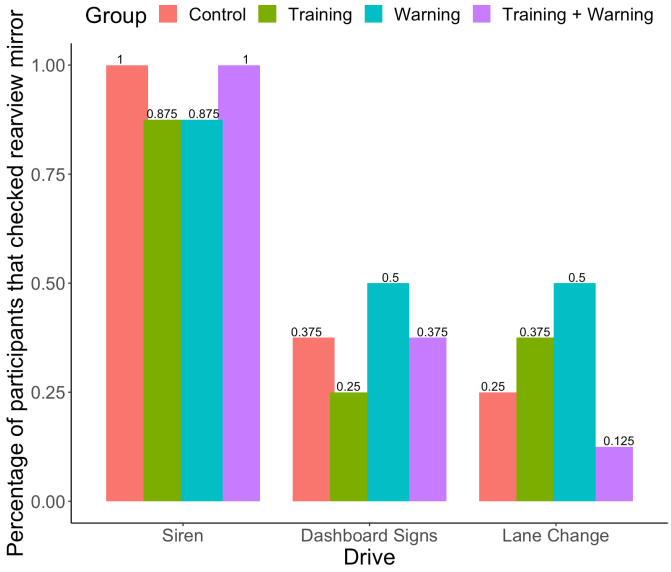


Figure 5: Percentage of participants who checked the rearview mirror, separated by group

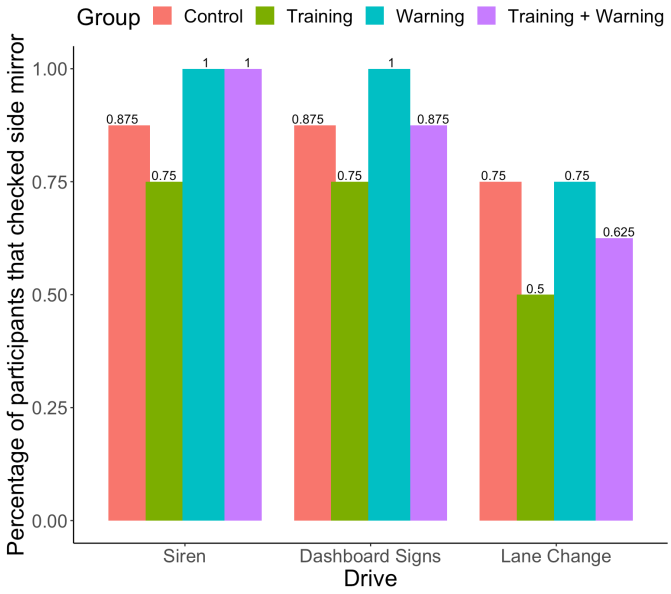


Figure 6: Percentage of participants who checked the side mirror, separated by group

Pull over

Figure 7 summarizes results for pulling over. The training and warning + training factors were significant. The training group, versus the control group, increases the log odds of pulling over by 1.89 ($\beta = 1.89$, $SE = 0.66$, z-score = 2.85, $p < 0.01$). The training + warning group, as compared to the control group, increases the log odds of pulling over by 3.95 ($\beta = 3.95$, $SE = 1.13$, z-score = 3.49, $p < 0.01$). The goodness of fit test was not significant ($p = 0.55$), implying that the model fit the data.

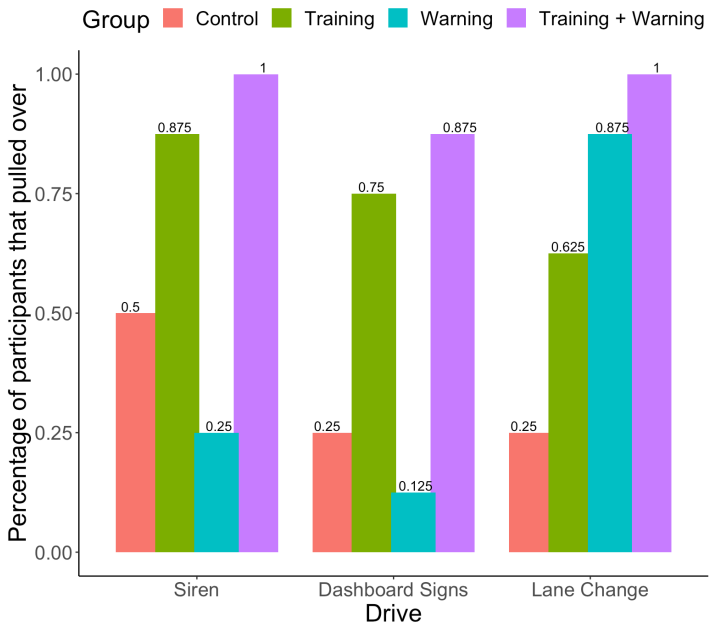


Figure 7: Percentage of participants who pulled over, separated by group

DISCUSSION

The objective of this study was to investigate how drivers respond to cyberattacks and to determine if training and warning systems affect drivers' responses to cyberattacks. We conducted a simulator study with 32 participants wherein some drivers received training on how to respond to cyberattacks and some drivers received warning messages (on the dashboard) about a cyberattack. Participants experienced three cyberattacks of differing severity levels.

Of the 11 behaviors that were examined, significant differences between the groups and drivers were only exhibited among four behaviors: looking at the dashboard for warning messages, checking the rearview mirror, checking the side view mirror, and pulling over. Those who received warning messages viewed them whenever they appeared. When participants heard a siren similar to an emergency vehicle, many checked their rearview mirrors, presumably to see if there was an emergency vehicle behind them. Similarly, when the vehicle began to abruptly change lanes by itself, participants were less likely to check the side view mirror. With respect to pulling over when a cybersecurity event occurred, those who received any form of training were much more likely to pull over, regardless of the scenario. Pulling over, for most participants, concluded the drive as they put the car in park. However, in the Sirens scenario, some participants pulled over, waited until the sirens stopped, continued to drive, but pulled over again once the sirens restarted.

Implications from this indicate the utility of training for improving drivers' responses to cyberattacks. Even a short training session– our training was approximately 10 minutes – leads drivers to be more cautious when their vehicle behaves unexpectedly. Providing simple messages on the dashboard capture drivers' attention, but do not necessarily lead to a change in behavior. There were stark differences in how drivers responded to cyberattacks across the scenarios: the sound of emergency sirens leads drivers to check their rearview and side mirrors much more so than other scenarios.

Though this study highlighted important findings when it comes to drivers' responses to cyberattacks, there are limitations and opportunities for future work. First, when coding participant videos, the researcher had to accommodate for a limited field of view. Future work should consider combining video data with driving behavior data (e.g., vehicle speed) to ascertain drivers' responses. The lack of an effect for warnings indicates they can be improved. Relatedly, a larger study with more participants and more cybersecurity events would allow for greater generalizability. Last, drivers in this study were young; future work can consider a different driving demographic, particularly those with more driving experience or who drive a vehicle on a day to day basis (e.g., for work).

REFERENCES

Baldwin, C. L., & Lewis, B. A. (2014). Perceived urgency mapping across modalities within a driving context. Applied Ergonomics, 45(5), 1270–1277. https://doi.org/10.1016/j.apergo.2013.05.002

Classen, S., Winter, S. M., Velozo, C. A., Bédard, M., Lanford, D. N., Brumback, B., & Lutz, B. J. (2010). Item Development and Validity Testing for a Self- and Proxy Report: The Safe Driving Behavior Measure. *The American Journal of Occupational Therapy*, *64*(2), 296–305. https://doi.org/10.5014/ajot.64.2.296

Cranor, L. F. (2008). *A Framework for Reasoning About the Human in the Loop*. 15.

Eiza, M. H., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, *12*(2), 45–51.

Garcia, F. D., Oswald, D., Kasper, T., & Pavlidès, P. (2016). *Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems*. 17.

Hodge, C., Hauck, K., Gupta, S., & Bennett, J. C. (2019). *Vehicle Cybersecurity Threats and Mitigation Approaches* (No. NREL/TP-5400-74247). Golden, CO (United States): National Renewable Energy Lab.(NREL). https://doi.org/10.2172/1559930

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., … Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. *2010 IEEE Symposium on Security and Privacy*, 447–462. Oakland, CA, USA: IEEE. https://doi.org/10.1109/SP.2010.34

Larson, U. E., & Nilsson, D. K. (2008). Securing vehicles against cyber attacks. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead - CSIIRW '08*, 1. Oak Ridge, Tennessee: ACM Press. https://doi.org/10.1145/1413140.1413174

McCarthy, C., Harnett, K., & Carter, A. (2014). Characterization of potential security threats in modern automobiles: A composite modeling approach (No. DOT HS 812 074). National Highway Traffic Safety Administration. (United States).

Petit, J., & Shladover, S. E. (2014). Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 1–11. https://doi.org/10.1109/TITS.2014.2342271

Wogalter, M., & Mayhorn, C. (2005). Providing cognitive support with technology-based warning systems. Ergonomics, 48(5), 522–533. https://doi.org/10.1080/00140130400029258

Wolf, M., Weimerskirch, A., & Wollinger, T. (2007). State of the Art: Embedding Security in Vehicles. *EURASIP Journal on Embedded Systems*, *2007*, 1–16. https://doi.org/10.1155/2007/74706

Zhang, F., Petit, J., & Roberts, S. C. (2019). A Simulator Study on Drivers' Response and Perception Towards Vehicle Cyberattacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 1498–1502. https://doi.org/10.1177/1071181319631310