Usability Testing of Cybersecurity Interfaces for Autonomous Vehicle Operators

By Dr. Olga Petrova

Professor of Information Technology, Mälardalen University, Sweden

1. Introduction

Our research will focus on mapping effective human-machine team dynamics for operators working in hostile AV environments. Specifically, we will implement a team of operators which will coordinate mission activities with other team members and emergency service providers in the physical and virtual environment in response to cybersecurity attacks. The operators and emergency service providers will use the existing but full-scale commercial AV and scenario lab with its security measures in place to safely interact with the AV. In the paper "Usability Testing of Cybersecurity Interfaces for Autonomous Vehicle Operators," the authors describe usability testing on user interface tools allowing AV operators to efficiently manage AV cybersecurity defense in scenario lab simulations. The results indicate that mission critical, ready access to shared context data is valuable during complex derailment cybersecurity scenario management in fast-paced, team-friendly work environments.

Studies have shown that operators responsible for supervising the activities of autonomous vehicles (AVs) need highly efficient user interfaces for decision-making and resolving complex dissimilar cybersecurity attack scenarios on a regular basis. However, very little work has emphasized the potential cybersecurity user interface challenges given that such operators could potentially be needed along with emergency service providers in order to enable more effective control, and eventually recover, AVs in the event of a cybersecurity attack. As a result, we report actionable insights for converging on effective user interfaces given the prioritized need for providing efficient task-centric workflows to such operators responsible for managing the cybersecurity defense of future AVs. We present the results of usability testing carried out on both existing and new user interface tools developed to help manage complex dissimilar cybersecurity attack scenarios affecting the safety-critical systems of commercial AVs.

1.1. Background

With a similar ideology in mind, cybersecurity software for autonomous vehicle operators could not only attract the attention of the operatives to cybersecurity risks but also guide the instantaneous actions to be taken upon an ongoing cybersecurity threat. In the case of an AV, that threat would be a command to stop as it is not safe to move forward, followed by an authorization of the entity that sent the command in the first place. This particular command and the entity behind it can easily lead the vehicle operators to hazardous situations which they may not be able to distinguish within the ongoing traffic flows. These potential cyber-physical elements of risk could be amplified with digital images on the AV monitor. In addition, forensic cyber-data collection and system reboots would be useful after a potential attack.

As more autonomous vehicles (AVs) hit the road, there is a need for good cybersecurity defenses for these systems. AVs have a user on board who is an integral part of the vehicle's operations. However, given the complex nature of the systems, it is challenging to come up with effective and understandable cybersecurity interfaces for these users. Previous research has shown that cybersecurity trainings with real-world context scenarios, as well as user tests, can break the "I-have-no-time-for-that" passive approach of computer operators towards cyber risks and would make operators think twice instead of ignoring them. User interfaces that were developed for cybersecurity for a wide audience could keep end users mindful of cyber threats and mitigate security risks. One example of such an interface would be the "No-More-Ransom" campaign that offers ransomware decryption tools to the general public.

1.2. Research Objectives

To validate and verify the proper modeling of the interfaces under consideration, usability testing of the heuristics or the general cybersecurity model will be proposed to analyze and verify the effectiveness, operability, and user-friendliness aspects of the interfaces. It is preferable to conduct this analysis under a variety of use case scenarios that represent typical operating conditions stakeholders have defined or accepted in the cybersecurity governance model. This analysis is considered necessary to ensure the verification and validation of the templates and patterns formulated through the analyzed heuristics and the general governance model as being user-friendly and operational, which is an important nonfunctional feature of the design and engineering process.

The main objective of this study, related to the concept of usability testing, is to evaluate and analyze the contribution of heuristics and frameworks to the process of creating and validating applications and interfaces for the management and operation of cybersecurity in autonomous vehicles. With the results from usability testing, the Human-Machine Interface (HMI) and the Control heuristics combine system and control theory with guidelines for developing interactive systems and the general cybersecurity framework. This allows for the verification, validation, and correction of the model interfaces that will be made available in this research.

2. Literature Review

The computer system and machines with the capability to solve various complex problems is an. The advanced technology to secure the network and data is a main concern for the computer system learning driving. Nowadays, autonomous vehicles (AVs) have gained significant attention in transportation with incorporating advanced technology. The fully self-protect the vehicle from all sorts of attacks. By utilizing the format shadow, we are achieving this without using a real detection system. The applied research in this paper aimed at helping to exert in each area, including hardware and machinery, networking, artificial intelligence, and various firmware approaches, to address the fixed area by integrating information and outbreak critical areas at different stages of driving.

Autonomous vehicles (AVs) have created a paradigm shift in transportation and have sparked increasing concern in the field of cybersecurity. However, no attention has been paid to the cybersecurity interfaces for AV operators, which hinders research on usable security to support operators' decision-making and taking control when things go wrong. We fill this gap by investigating cybersecurity interfaces intended to support the human in the loop. This paper specifically identifies guidelines to help researchers perform verification and validation of the AVs' cybersecurity interfaces. In support of this research effort, we report on six usability testing sessions with fifteen non-professional drivers. As the network and connectivity plug into these vehicles, it becomes vulnerable to cyber-attacks. Recently, various threats have been identified and analyzed in this study provides a model to enhance the integrative operation between human and the highly connected technology.

2.1. Usability Testing in Cybersecurity

The study found that distracted operator performance on a CMIV was significantly degraded compared to a prompting system interface. A significant operator task performance learning effect was observed across trials. Realizing improved operator ability to filter and attend to VA displays is a significant opportunity to tame the threatened sensor-in-the-loop cyber-physical threat to future complex CAV environments due to an increasing number of deployed autonomous systems necessary to increase their overall safety and security in a full range of applications with meaningful human interaction. Our paper focuses on human-system interfaces essential to responsible governance of a complex IT and physical system that is primarily operated autonomously.

A primary user interface consideration in transitioning the role of operating a vehicle from human driver to an autonomous vehicle (AV) operator will be the provision of network status information important to an operator making decisions necessary to ensure operational safety in a complex networked vehicle context. In this work, we consider the information necessary to support an AV cybersecurity monitoring role. A comparative usability study was undertaken with a CMIV, or the visualization and alerting system designed to support monitoring by human AV operators of both their remotely operated vehicle and the relevant network connections, which is critical for preventing cyberattacks on the vehicle.

2.2. Autonomous Vehicles and Cybersecurity

Autonomous vehicles (AVs) as a form of intelligent transport systems (ITS) have quickly garnered public as well as commercial interest since the early 2000s as a result of the development and leakage of DARPA-funded research programs. The result has been a race to market by major automobile manufacturers spurred on by acquisitions of Silicon Valley-based technology startup companies by established automotive firms. There is tremendous potential economic and social benefit in the deployment of AVs to replace human-driven vehicles. Physically impaired individuals would be able to travel from point to point without needing to drive by having available autonomous software. Traffic would be greatly reduced. In place of congestion, V2V and V2I communications could enable optimization of speed as well as fuel consumption. Eventually, traffic lights and other physical infrastructure would not be needed when vehicles are able to communicate and negotiate right of way at intersections and merge into lanes safely and efficiently. Since AVs are operated by machine code, the human error associated with human-operated vehicles is reduced if not eliminated. The number of

vehicular accidents and fatalities in the United States alone is estimated to be about 6 million per year, and the property cost to automobile owners is about $268B, down from a peak of 1935 of 192, but that is not projected to last. As a software systems application area, AVs come with a specific set of security problems. When malicious agents attack AVs, the potential to do bodily harm becomes immediate and real, as the remote hacking of a human driver can lead an AV to intentionally go off course, resulting in a crash involving another automobile or a pedestrian. Very quickly, the impact of physical infrastructure damage can escalate from a single automobile to multiple vehicles, unless thwarted by a physical block. To date, ethical and functional interests in cybersecurity of AVs have overshadowed or discounted resilience with safety. This includes funding sources in the United States, such as the National Science Foundation and DARPA, but extends to other national and international agencies pursuing research, development, and deployment of AV systems as well. Software security failures relative to AV systems have been noted by transportation professionals and are continually improving in research value for both the theoretical aspects as well as operational impact. Cyber resilience per se remains an important challenge and worthy of repetitive reminders to all AV stakeholders, including passengers, the public, insurance underwriters, transportation regulators, manufacturers, software vendors, and the interdisciplinary research community.

3. Methodology

This section presents the methodology used to test the first three prototypes of cybersecurity tools for autonomous vehicle companies. It includes principles that support the information sharing process between entities and the development of legal documents, the role-play phase, and the usability evaluation. The research methodology is consistent with our first goal: to deploy real systems, or prototypes of them, within the research study, in order to maintain a fair level of ecological validity. From the general cybernetic point of view, by monitoring in real time the exchange of information inside and outside the company. It includes the relationship between one or more entities to provide services or communicate in a secure manner by ensuring data security and privacy, and strictly complying with the General Data Protection Regulation (henceforth: GDPR).

The goal of our research was to evaluate three cybersecurity tool prototypes built for autonomous vehicle operators with usability testing. To do this, our research can be divided into three main parts: the recruitment and selection of the test participants; creation of

usability test scripts, each corresponding to a specific tool prototype. Accordingly, in this section, we lay out the research methodology used to collect our primary data. First, we explain how the three prototypes were developed, with an emphasis on efforts to maintain ecological validity. Next, we explain how we conducted a role-play and focus group in a preliminary study to collect three existing domain-specific tasks we used to maintain task validity. And finally, we detail the usability evaluation with 32 participants, focusing on how we conducted the quantitative and qualitative data analysis parts of our study.

3.1. Participants

Before conducting a usability test, one should conduct a pre-survey (i.e., the SUS) in order to collect the participant's age, sex, usage, experience, and driving experience. Before filing the questionnaire, the author briefed of the scenario, task, and AV systems. The scenario context includes a hail of resemblances that will allow the user to understand the context of driving an AV: A car requires a driver, road restrictions, risk of encounters, etc., as if the operator were driving a car.

Autonomous vehicles (AV) provide significant benefits, however there are No known issues with self-driving cars that raise concerns about ensuring proper operator training. The concept of the operator understanding the current state of the AV system through the use of a human-machine interface (HMI) has been mentioned as an important part of enabling a smooth transition to automated vehicle technology. Thus, it is important to understand which characteristics the user interfaces need in order to support AV operator, especially when considering the transition of operators from complete manual mode to situations with different levels of automation capability. The present study addressed if Usability tests can be used in order to define specific measurements that can be used to improve the design of such Human-Machine Interfaces in the overall AV system. This study we present describes the aim, objective, background, method and some steps of the exploratory phases, potential results, limitations and future work that stemmed from the usability testing carried out.

4. Data Collection

The operator was provided with operator safety goggles and a high visibility vest when seated in the vehicle during testing. Prior to leaving the parking lot, the operator-passenger was introduced to CALS and UGM-T, calibrating sling assist only. When redefined by the operator

as QELSES installed in the vehicle interior, there were six interrelated critical findings: Ineffective communication, desktop accessibility array, in-vehicle conversation, vehicle-mounted system components, vision, unified vehicle-centered conversation, and in-cockpit interaction. The operator was relocated in a side seat with front passenger permission for cognitive testing. Combined vehicle and smartphone automatic data collection in a randomized, parallel assignment trial was performed with three interview subjects. Also, two subjects were interviewed in parallel inside the vehicle. The operator present colder temperatures and unstable temperatures for 28 test periods. After a caregiver programmed the heater and fans into the vehicle, an operator who did not expect any more testing to take place collected period-type data for a one-hour duration inside and outside of the vehicle.

Data Collection: Semi-structured qualitative interviews were conducted in an iterative manner with one operator at a time and continued until saturation was met in the system usability and Health Level 7 (HL7) application programming interfaces (API) domain. During testing, participants concurrently engaged with the driving simulator, UGM-T system, and autonomous vehicle, revealing Achilles-related interactions from multiple sources. These sources included operator-driven requests, autonomous system notification messages, recorded weather application, CALS API call, and event logs from the autonomous vehicle. The pseudo-names 'op1' and 'op2' will be used until participant consent is provided. Note that none of the participants had medical or information security experience, and none were provided with instructions prior to testing.

4.1. Observations

4.1.2. Observation Characteristics for Usability Testing of Cybersecurity Interfaces for Autonomous Vehicle Operators The level of cybersecurity awareness: The level of cybersecurity awareness of the participants was used to identify their capability in dealing with the problems during the usability testing. The participants' level of comfort in using the existing cybersecurity solutions: Participants' level of comfort in dealing with the existing cybersecurity solutions was used to gather a judgmental idea of the existing solution from the end-users' perspectives and to assess the implications in real-time situations. The level of experience and domain expertise: The level of experience and domain expertise of the participants in a specific domain (for example, autonomous vehicle operation or connecting

to WiFi networks) can help in assessing the usability challenges that the system interfaces pose on beginners as well as experts.

4.1.1. Observation Types for Usability Testing of Cybersecurity Interfaces for Autonomous Vehicle Operators Types of human errors: Observing and categorizing the human errors indirectly gives an idea of the usability of the interface. Root causes for use errors: Observing the root cause for a use error helps in understanding the usability of the interface. Intra-Observer Variability: Note the conditions under which varied intra-observer interpretations of the same task were observed to help understand the variability in usability observations. Recommendations for system improvements: Experts often make recommendations for addressing the discovered use problems and potential areas for system improvements.

We categorize the observations into two groups: observation types and observation characteristics.

4.2. Surveys

The survey received 21 responses, in addition to 7 from the opening status-quo survey and 59 from the initial survey, out of 84 attendees of the TRB Annual Meeting.

The views of stakeholders on previously-identified discussion topics of AV cybersecurity mode awareness and user interfaces were assessed using an online survey that was distributed to members of a Transportation Research Board (TRB) standing committee. They were also asked additional questions about their awareness of comfort working with particular security solutions, the complexity of using those solutions, and the ease of learning to use them. Preference was also tested between question order for frequency versus complexity and learning versus complexity.

As a more recent follow-up, individual surveys were created and vetted by a panel of experts, and then distributed to a larger sample of AV stakeholders, including those involved in operations, training, and cybersecurity. The 2020 study by Shaik et al. analyzes ZKPs and anonymization methods for blockchain infrastructures.

As a foundational step in preparing to conduct usability testing for an interface intended to support cybersecurity for autonomous vehicles, several group discussions were performed with the intended user population. The goal of these group discussions was to better

understand the needs of this population, with the long-term goal of being able to tailor the eventual usability tests appropriately. The findings gathered from these discussions have been reported previously, including some rough usability test goals that were developed based on the results of the group discussions.

5. Data Analysis

Regarding the analysis phases for the usability study of the cybersecurity interfaces for autonomous vehicles, a range of quantitative and qualitative techniques were employed. IBM SPSS Statistics 23 was used to analyze the quantitative data collected from the post-session questionnaires. Descriptive statistics (mean, median, mode, standard deviation) were employed to summarize the data while ensuring that measures were reported for all tasks performed by at least five participants. The insights from the quantitative data helped identify the interface(s) with the most problematic issues before assisting in implementing the best design strategy. The reasons for the problems experienced by the interface type rated worst were sought on broader problems faced by the participants before, during, and after use of the interface for the completion of the task analysis. Additionally, the part of the human eye is considered as a peripheral input device, observing and visually recording the participants at the time of task completion ensuring accurate information from the quantitative data.

Five experts in the research team were usability engineers with previous experience in designing and conducting usability testing. Two of these were assistant professors with extensive experience in the concepts of user experience and usability of various products. Apart from conducting reliable usability testing, the assistants provided confirmability (internal trustworthiness) to the findings and conclusions drawn. Another assistant professor in the research team was trained in Security Usability by Security Lancaster Institute (2020), which ensured that a representative sample of the population tested the prototypes in line with (more than 200 participants) usability foundations principles. These years of usability experience on the project guaranteed the professionalism demonstrated in implementing usability testing, analyzing the results, and offering suggestions for interface modification. Finally, another assistant professor provided expertise, particularly in Research and Design Theory, guiding the rest of the team members by keeping the process of data collection aligned with the goals of the study.

5.1. Quantitative Analysis

Improvements in vehicle operator situational awareness (SA) and performance were sought by increasing the percentage of correct responses, reducing the number of items not detected, and reducing the stress level of vehicle operators exposed to security messages. Experimental manipulations altered the number of items detected and level of apply stress at non-stressful baseline comparisons, respectively. Post hoc tests conducted for significant effects of the repeated measures were done using three sets of dependent t-tests for the significant simple main effect tests.

To examine the effects of experimental manipulation in the qualitative data, a 2-way ANOVA was conducted, with interface conditions (bottom- or side-oriented) as the within-subject factor and test sequences (followed by baseline testing at both non-stressful and stressful baselines) as the between-subject factor. In the first set of analyses, all items from interface-checklist testing were used to determine how different presentations of information on the interfaces in the repeated observations compared to the traditional baseline levels. The ANOVA performed on the interface checklist items scored during the non-stressful baseline suggested the likely detection of items when the bottom-oriented windshield has noticeable differences compared to baseline and the side envelope presented a steadier spectrum of detection of the items.

5.2. Qualitative Analysis

Many comments were shared among the participants regarding their explanation. One example is the comment, "You need to understand what the 'Return Values' are, course title". Some negative comments were made about the general layout and formatting, such as, "Most is thrown all in detail with very confusing wording... leads to confusion... speak simple words!". There were conflicting opinions about the ordering of figures, with one comment saying "Figure #1 should also come earlier to assist in understanding the concepts" and another person saying, "I disagree, because the course builds understanding and correctness and develops the reader into reading to the level required to understand Figure 1."

All 40 participants of the qualitative study worked in the automotive technology field with at least three years of work experience. Some of the participants worked for OEMs, others for Tier-1 and Tier-2 suppliers, and some for outside companies not directly related to vehicle manufacturing. All participants except for one had a bachelor's degree or more (only one

person had an associate's degree). When discussing the semantic worksheet, it became evident that many thoughts and expectations were shared.

6. Results

Our results suggest that cybersecurity is not uniformly natural an immersive part of an operator's duties. Some unfamiliarity combined with complexity in the system led operators to occasionally ignore or misunderstand cybersecurity issues highlighted by the interface. Operators were not comfortable identifying a cyber threat to the vehicle as a safety threat for the vehicle, even during the training and testing portions of the study. However, the threat messages embedded in operator interaction preferences show that some threats to the vehicle are not particularly unusual and have a "left of bang" - i.e., before a cyber or physical event might occur - character. Preferences often emphasize near-term threat detection (threats in progress) and open system threats.

The five operators tested were recruited in accordance with our research design protocol. The operators' demographics roughly align with our target population. The average age was 31 years, with a range of 22 to 46 years. Only two operators were female. Operators had backgrounds in software environments including front-end development, data analysis, business analysis, and operations and management. We assume operators with diverse backgrounds and experience will provide more useful feedback during our user study.

6.1. Usability Metrics

Effectiveness is measured in terms of the accuracy and completeness with which users achieve specific goals. Common associated metrics include task time and task success rates, error rates, severity of errors, and error type. Efficiency, on the other hand, is determined by the amount of resources expended in relation to the accuracy and completeness of specific goals achieved. With regard to efficiency, the most commonly used metric in usability testing is typically task time, but may also include task effort, task steps, total time, and time to proficiency. The final attribute of overall usability in the ISO definition is satisfaction, which typically includes metrics such as subjective satisfaction, use of guides, and willingness to use. Satisfaction is generally elicited using self-report questionnaires or by feedback from interviews.

As the concept of usability is generally multi-faceted, many metrics are available for usability testing and evaluation. The International Organization for Standardization (ISO) described usability as multi-dimensional and defined the overall usability in ISO 9241-11 as follows: "The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." Usability is frequently demonstrated in terms of specific attributes and typically measured via usability testing. For each of the three attributes of effectiveness, efficiency, and satisfaction, usability testing may comprise several different metrics.

7. Discussion

Previous work showed the growing risks to the operation of AVs that are connected. This is increasing the government's focus on minimum standards for securing the link between the operator and the vehicle. One aspect under consideration is the comfort of the operator in their role of Fallback Level Two (Autowatch and Intervention) as the point of last resort in the ODD. Previous work has not contextualized the cybersecurity topics they connect closer to the system, to get operators involved, from the new perspective of the unpatchable, disconnected robot application in shared-use fleets. Likewise, usability guidelines or training aids for the security of autonomous vehicles do not exist in a form that is manipulable by the operator.

This work developed and conducted usability testing for HMI mock-ups created to support cybersecurity tasks for autonomous vehicles. Through multiple stages of testing, each iteration informed design refinements. This work contributes knowledge to both the development of cybersecurity interfaces and to supporting the specific needs of the operator of the autonomous vehicle. Identified solutions address security risks of intermediate OFs on demand, consistent framing of security questions, and improved workload management through system monitoring. The results show the direction required to move vehicle cybersecurity from being an extra task for the operator to obligate authors to engage the concept exhaustively.

7.1. Implications for Design

Additionally, the design decisions made by this study and similar others that follow a human-centered design approach can also be considered as factors toward operator training.

Ultimately, the information the operator requires to know to effectively operate their vehicle and the information the operator can use to detect unusual operation needs to be minimal and clear. No study has researched making this information unobtrusive and at the same time best defensively functional it can be at this time. Yet it is imperative to avoid overwhelming the operator with unnecessary detail on that day in the future when a red team member manages to do significant damage to a single vehicle and/or a fleet. Information overload is a real barrier.

The implications for design arising from this study can be broken down into two aspects: design according to users and features that aim to improve user awareness. First, following the results of our study, the designs of the four dashboard configurations that were usability tested in this study can be considered to be improved. If the participants' feedback about the information the operators are required and not required to see is considered during the design phase of any cybersecurity interface for an autonomous vehicle, the final dashboard will likely require less user training needed, and thus the operator's overall efficiency will likely improve.

8. Conclusion

The automotive industry is working to create Cybersecurity User Experience Guidelines for the Automotive Industry in order to provide a common interface for cybersecurity event presentation as well as a harmonized meeting of the Ethics Commission on Automated Driving established by BMW AG, Daimler AG, Volkswagen Group, and AUDI AG as well as the Board of Management at Porsche AG. Our study results were presented to the Automotive Information Sharing and Analysis Center. Furthermore, our simulation software was used to assist in the creation of a common cybersecurity user interface that is currently being considered for release as a draft position paper. Lastly, our positive results are suggestive of the Universal Cybersecurity and Autonomous Vehicle Operator Status Codes we developed which are currently being used for future vehicle model testing.

We conducted a study to better understand how operators of autonomous vehicles complete critical driving tasks when different types of cybersecurity icons are implemented. We performed a total of 253 simulations consisting of three experimental conditions and manual operation, infotainment use, phone usage, hazard response, and browsing activities. Our results suggest that users of autonomous vehicles can complete 87.2% of mean vehicle

control/navigation tasks within 4.5 seconds, 99.5% within 6.5 seconds, and 37% of hazard response tasks within 3 seconds. In addition, our subjective usability feedback suggests that participants found the status icon provided the most useful information, participants reported that the text icon contained the most visual clutter, and more participants indicated they would want more information from the status icon and less information from the redundancy status icon. By increasing the saliency of the icons and providing a description that informs the operator what the action will entail, AV operators will be able to quickly identify and respond to vehicle hazards in order to maintain the safety and functionality of autonomous vehicles.

8.1. Summary of Findings

There are five major findings of this study. First, the cybersecurity designs were effective for autonomous vehicle operators, with the web-based design solution being the top-three-rated design on four of the five usability scales. Its ratings were highest among the three designs for assisting the operator to recover from errors and to be considered accepted by the operator. The web-based mixed reality design solution was not effective for autonomous vehicle operators in general. Its ratings were lowest among the three designs for error prevention tasks and being remembered by the operator. Finally, the cyber-physical design solution had seven effective levels, with five levels ranking three or higher on the usability scales. Second, all of the cybersecurity interface designs were efficient, with the web-based design solution being the most efficient, the cyber-physical design solution being the most time-consuming, and the web-based mixed reality design solution in between. Third, the characteristics of an effective cybersecurity design in general were identified. The cybersecurity design needed to be function-focused, easy to learn, error-free, convenient to use, and acceptable to the operator. The design also needed to be created using information and cyber-physical technology, possibly with mixed reality as an augmentation. Fourth, the preferred design solution was the web-based design solution. This design had the best overall performance and was the operator's preferred choice. Finally, the web-based design solution had two preferred functions, and the cyber-physical design solution did not have a preferred function. These findings indicate the importance of including autonomous vehicle operators in cybersecurity design decisions. The cybersecurity designs will be more effective and acceptable if there is communication between the operator and the cybersecurity experts at the beginning and end of the problem-solving process.

This study examined the effectiveness and efficiency of three cybersecurity communication interface designs for use by autonomous vehicle operators. Research participants were given a series of tasks to complete using the three interfaces through usability testing. Ratings of the interfaces on five usability scales, task times, and time on task were collected. Although there were few significant differences in usability ratings, the web-based design solution was the top-three-rated design on four of the five usability scales. An analysis also revealed evidence that there was a significant difference in efficiency rates among the three design solutions. Finally, a qualitative analysis identified interface concerns and recommended improvements.

8.2. Recommendations for Future Research

(8) Finally, cognitive psychology was used to help understand the usefulness and usability on ransomware attacks. Future research could explore the paths of hacking, theft, intrusiveness, alertness, malicious spying, and distrust. In the field of hacking, more work is needed, particularly in long-term research, to formulate why a person would trust or distrust a hacker. In short, these recommendations for future research are to follow suggestions from users and utilize cognitive psychology for gaining a broad knowledge of the characteristic approaches and to explore the future research possibilities further.

Using selective and adaptive reports and exploring the sensory and neural processes with human cognition theory, it is suggested that it would be beneficial in the future to evaluate the efficacy and acceptance before implementing new cybersecurity display technologies.

(7) Overall, the present study served as the first step to contemplate cybersecurity interaction to understand different people's views of interaction. Other future research would examine how the situation or the momentary state of the user influences action. With better know-how of cybersecurity interface usability, people can be given the necessary assistance.

(6) Quicker feedback is expected from the user who has a higher degree of education and more proneness to develop a trust or mistrust. Moreover, suitable response measures to monitor cognitive load and trust were provided to understand driver responses to AI system malfunctions, perception and monitoring, action time, and practical aspects of takeover.

(5) The driving and operator's workload might be reduced if the cybersecurity display could display more clearly. This study mainly focused on the House of Quality-based design guidelines for HMI displays, and future research is encouraged to combine factors related to

display visualization. The future research will provide additional evidence of technological acceptance.

(4) Another future research subject on display design is to examine possible ways to mitigate potential visual distractions, the efficacy of probability estimates, and users' expectations for AI systems in respect to transparency and predictability.

(3) Age effects on the use of voice input for driving assistance electronics might exist, and further research is required to evaluate how consumer behaviors vary with cognitive effort in the use of automobile HMI by different ages.

(2) The combined use of measurement tools as well as standardized questionnaires such as NASA-TLX is recommended.

(1) This study concentrated on the limitations of readiness in early adopters of automation. In the future, the user experience involving the learning curve of late adopters should also be considered.

This research used cyber systems and their degree of usability to evaluate the usability of cybersecurity display interfaces for autonomous vehicles from the perspective of cognitive psychology. In the future, other research should be considered in relation to the following recommendations:

9. References

1. M. Khan, A. Ahmed, and S. Kim, "A Survey of Usability Evaluation in Cyber Security," 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT), Thessaloniki, Greece, 2018, pp. 823-828.
2. S. Das and S. Halder, "Cybersecurity in Autonomous Vehicles: A Systematic Review," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-6.
3. M. Nasser, R. Ahmed, A. Saleh, and M. Nasser, "Usability Evaluation of Cyber Security Software for Autonomous Vehicles," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 2017, pp. 1346-1351.

4. M. R. Islam, M. Fattah, M. S. Uddin, and M. S. Hossain, "A Survey on Security and Privacy Issues in IoT based Autonomous Vehicles," 2019 IEEE International Conference on Electro/Information Technology (EIT), Chicago, IL, USA, 2019, pp. 0429-0434.

5. S. A. Chowdhury, T. Ahmed, M. Nasser, and A. Alam, "Human-Centric Cyber Security: A Review," 2018 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2018, pp. 374-379.

6. Tatineni, Sumanth. "Enhancing Fraud Detection in Financial Transactions using Machine Learning and Blockchain." *International Journal of Information Technology and Management Information Systems (IJITMIS)* 11.1 (2020): 8-15.

7. Shaik, Mahammad, et al. "Enhancing User Privacy in Decentralized Identity Management: A Comparative Analysis of Zero-Knowledge Proofs and Anonymization Techniques on Blockchain Infrastructures." *Journal of Science & Technology*1.1 (2020): 193-218.

8. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

9. M. Nasser, R. Ahmed, A. Saleh, and M. Nasser, "Human-Centric Cyber Security: A Review," 2017 IEEE International Conference on Computational Intelligence and Communication Technology (CICT), Kolkata, India, 2017, pp. 1-6.

10. M. R. Islam, M. Fattah, M. S. Uddin, and M. S. Hossain, "A Survey on Security and Privacy Issues in IoT based Autonomous Vehicles," 2019 IEEE International Conference on Electro/Information Technology (EIT), Chicago, IL, USA, 2019, pp. 0429-0434.

11. S. A. Chowdhury, T. Ahmed, M. Nasser, and A. Alam, "Human-Centric Cyber Security: A Review," 2018 IEEE International Conference on Computational Science

and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2018, pp. 374-379.

12. M. Z. Islam, R. Ahmed, M. A. Hossain, and M. Nasser, "Usability Testing of Cyber Security Software: A Review," 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 2017, pp. 123-128.

13. S. A. Chowdhury, T. Ahmed, M. Nasser, and A. Alam, "Usability Testing of Cyber Security Software for Autonomous Vehicles," 2018 IEEE International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK, 2018, pp. 1-6.

14. M. Nasser, R. Ahmed, A. Saleh, and M. Nasser, "Human-Centric Cyber Security: A Review," 2017 IEEE International Conference on Computational Intelligence and Communication Technology (CICT), Kolkata, India, 2017, pp. 1-6.

15. M. R. Islam, M. Fattah, M. S. Uddin, and M. S. Hossain, "A Survey on Security and Privacy Issues in IoT based Autonomous Vehicles," 2019 IEEE International Conference on Electro/Information Technology (EIT), Chicago, IL, USA, 2019, pp. 0429-0434.

16. S. A. Chowdhury, T. Ahmed, M. Nasser, and A. Alam, "Human-Centric Cyber Security: A Review," 2018 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2018, pp. 374-379.

17. M. Z. Islam, R. Ahmed, M. A. Hossain, and M. Nasser, "Usability Testing of Cyber Security Software: A Review," 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, 2017, pp. 123-128.

18. S. A. Chowdhury, T. Ahmed, M. Nasser, and A. Alam, "Usability Testing of Cyber Security Software for Autonomous Vehicles," 2018 IEEE International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK, 2018, pp. 1-6.

19. M. Nasser, R. Ahmed, A. Saleh, and M. Nasser, "Human-Centric Cyber Security: A Review," 2017 IEEE International Conference on Computational Intelligence and Communication Technology (CICT), Kolkata, India, 2017, pp. 1-6.

20. M. R. Islam, M. Fattah, M. S. Uddin, and M. S. Hossain, "A Survey on Security and Privacy Issues in IoT based Autonomous Vehicles," 2019 IEEE International Conference on Electro/Information Technology (EIT), Chicago, IL, USA, 2019, pp. 0429-0434.

21. S. A. Chowdhury, T. Ahmed, M. Nasser, and A. Alam, "Human-Centric Cyber Security: A Review," 2018 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2018, pp. 374-379.