Research on Companies' Perception of Risk of Cyber Security Attacks on Autonomous Vehicles

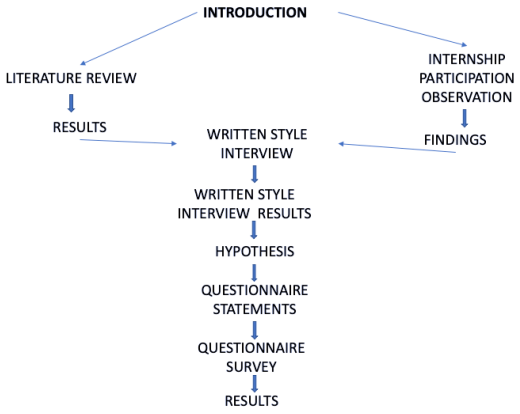
51836701 Mamajiwala Burhan Yunus

First Supervisor Prof. Maeda Yasunobu
Second Supervisor Prof.Takahiro Hasegawa

1. INTRODUCTION

The development of autonomous vehicles technology has led to significant connectivity [1]. Today's society runs largely on technology. As a result, we are dependent on it. The way technology brings benefits, it also brings threats; by the very nature of the opportunity it presents, it becomes a focal point for cybercrime and cyber attacks. Hence protecting it is a major priority. The goal for this research is to find out companies' perceptions of cyber risk attacks on autonomous vehicles by designing written style interviews and questionnaires.
The flowchart depicted in Figure 1 below shows the overview of the work done in this study.

Figure 1 Overview of the work done in the study.



2. LITERATURE REVIEW

The aim of this research is to bridge the knowledge gap between expected level of cyber risk management and current situation in automotive companies and third parties. The table below shows the knowledge gap and the possible impact/risk outcomes [2].

Table 1 Knowledge gap and possible impact/risk outcomes.

Knowledge Gap ⇒	Possible Impact/Risk
Privacy of Personal information	Unauthorized access of user information. location and identifying information
Ownership of Data	Uncertainty needs to be cleared for ensuring data is only accessed by those who own/need it.
Lack of standardization	It is unclear to manufacturers and developers, how to most efficiently combine the efforts to finding risk and ensuring high security by research, where there is no general accepted standard for AV security
Lack of knowledge on security concerns	The control system and functions of AV can magnetize problems due to the incapability of handling internal network
Lack of knowledge about response to attack	Manufacturers may not have implemented reductions to handle attacks that have not been accounted for. Without knowledge about appropriate attack responses.
Lack of knowledge about VANET security	In order to physically harm or interrupt traffic, an attacker can intercept communication locally to other vehicles.
Lack of knowledge about vulnerabilities for ECU,GPS & sensors	Security measures that are implemented do not cover the vulnerabilities unless these areas are further explored. Vehicle users will be exposed to danger due to successful attacks performed.

3. WRITTEN STYLE INTERVIEW

To gather a professional viewpoint from cyber security experts a written style interview of 11 questions were designed and send to 6 cyber security specialist companies. The research focuses on the knowledge gap of risk perceptions between automotive manufacturing companies and third party companies. 25 hypotheses as a result were obtained from the written style interview. The hypotheses suppose that automotive companies and third party companies have different perception about the following 25 statements.

1. Automotive manufacturing companies prioritize the sensitive information lost in autonomous vehicles.
2. Cyber attackers attack the autonomous vehicle by compromising the performance of communication systems, for example, Vehicle to Vehicle (V2V) communication, Vehicle to Infrastructure (V2I) communication, and entertainment systems.
3. Denial-of-Service attacks prevent normal functioning in autonomous vehicles.
4. Ransomware attacks are important as a cyber risk in autonomous vehicles.
5. Edge computing reduces the risk of cyber security on the network connecting to autonomous vehicles.
6. Cyber attackers choose targets with a high potential value not requiring a lot of resources.
7. Cyber attackers cause loss-of-control of autonomous driving systems.
8. Autonomous vehicles can be a vector of stealing information from mobile devices.
9. Vehicle data spoofing is an important as a cyber risk in autonomous vehicles.
10. Vehicle to Infrastructure (V2I) communication targeted to compromise the infrastructure is dangerous as a cyber risk in autonomous driving systems
11. Malicious software installed through physical ac cess, e.g., diagnostic ports, is important as a cyber risk in autonomous vehicles.
12. Insurance fraud associated with autonomous driving cars is important as a cyber risk in autonomous vehicles.
13. Extortion of government authorities by cyber attackers on autonomous vehicles is an important as a cyber risk in autonomous vehicles.
14. Autonomous vehicles misread the existence of people or objects by the interference of threat actors.
15. ISO 21434 has an important role in cyber security on autonomous vehicles.
16. Automotive companies should implement higher cybersecurity standards for building reliance.
17. Responsibilities and liabilities of automotive manufacturing companies should be clearly defined.
18. Automotive manufacturing companies should train the cyber security teams, like SOC or CSIRT.
19.The role of accident investigation in cyber security risk management by the independent organization is important for autonomous vehicles
20. In autonomous vehicles, detection of cyber threats by real-time monitoring of vehicle performance and detection of small anomalies are required.

21. When the autonomous vehicle is not in control, Fail-safe systems should transit the autonomous vehicle to a safe state.
22.Automotive manufacturing companies should consider cyber security countermeasures like defense-in-depth design from designing process and production processes.
23. Countermeasures like access control, read only hard drive and filtering and re-routing are effective to protect autonomous vehicles from cyber threats.
24.To protect autonomous vehicles from cyber threats, risk management policies of automotive manufacturing companies are important.
25.Continuous updates of software are effective for risk management of autonomous driving cars against cyber threats.

4. QUESTIONNAIRE SURVEY FOR AUTOMOTIVE COMPANIES AND THIRD-PARTY COMPANIES

A questionnaire survey was conducted to understand the differences of the cyber risk perceptions between automotive and third-party companies. The questionnaire survey was sent to 100 third party companies (cyber security specialist companies) and 100 automotive companies (autonomous vehicle manufacturing companies). The survey period was conducted between May 6th 2021 – June 2nd 2021.

The summary of the questions is described as follows:

A) Asking companies to indicate the level of agreement for all 25 questionnaire statements
(Strongly disagree, disagree, neutral, agree, strongly agree and don't know)

B) Companies' opinion on the importance of cybersecurity risk of autonomous vehicles

C) Companies' products and services, number of employees, capital amount, country and addition comments about the survey. From the questionnaire survey, a result of 77 company responses (out of 200 companies) were received. 44 responses were from automotive companies and 33 responses were from third party companies. A response rate of 38.5 % was achieved. By applying basic statistics and t-test to the questionnaire survey responses, Table 2 was produced.

Table 2 Confirmation of result using t-test.

Questions	Automotive [Mean]	Third Party [Mean]	T- Value
Q1-1	3.81	3.48	1.60
Q1-2	4.24	3.80	**2.32***
Q1-3	3.76	4.00	-1.60
Q1-4	4.04	4.17	-0.70
Q1-5	4.02	3.56	**2.70***
Q1-6	3.89	4.30	**-2.54***
Q1-7	4.02	3.90	0.69
Q1-8	3.91	3.60	1.41
Q1-9	4.04	3.86	1.05
Q1-10	4.06	4.10	-0.19
Q1-11	4.06	4.14	-0.44
Q1-12	3.70	3.56	0.75
Q1-13	3.84	3.93	-0.43
Q1-14	3.96	4.24	-1.99
Q1-15	4.18	3.89	1.60
Q1-16	3.87	4.03	-1.01
Q1-17	3.98	4.17	-1.02
Q1-18	4.00	4.07	-0.38
Q1-19	3.87	4.00	-0.73
Q1-20	4.00	4.07	-0.43
Q1-21	4.06	4.00	0.36
Q1-22	3.87	4.17	-1.95
Q1-23	3.98	3.83	0.89
Q1-24	4.09	4.17	-0.58
Q1-25	4.17	4.28	-0.65

* Denotes SIGNIFICANT
* Means $p<0.05$.

5. DISCUSISON

The outcome of the questionnaire survey is summarized in table 2 where Q1-2, Q1-5 & Q1-6 were resulted to be significant. Out of 25 hypotheses, 3 hypotheses were accepted, and 22 hypotheses were rejected. *Accepted alternative hypothesis*: For Q1-2 and Q1-5 the mean of automotive companies displays a greater value than the third-party companies whereas for Q1-6 the mean of third-party companies displays a greater value than the automotive companies. These differences suggest knowledge gaps of cyber risk perceptions are present between automotive and third-party companies. These differences emerged as automotive companies and third-party companies do not have a balance in the exchange of information for the subject areas (Q1-2, Q1-5 and Q1-6). *Rejected alternative hypothesis: The* result shows 22 hypotheses were rejected. The reason being there is no knowledge gap present for the rejected hypothesis subject areas.

6. CONCLUSION

As a result, differences in 3 hypotheses were found. The cybersecurity risk perceptions of different companies were analysed and studied in this research. From the result, it suggests that out of 25 hypothesis 3 were significant (Q1-2, Q1-6 & Q1-5). The result suggests that there are differences present because of the differences of fundamental way-of-thinking between automotive companies and third-party companies. Furthermore, the result also suggests that Automotive companies and third-party companies should exchange more knowledge for the possibilities of cyber attackers to attack autonomous vehicles for the following subject areas:

A) Compromising the performance of communication systems which include V2V (vehicle to vehicle), V2I (vehicle to infrastructure) and entertainment systems. (corresponds to Q1-2)
B) Edge computing systems. (corresponds to Q1-5)
C) Choosing targets with a high potential value do not require a lot of resources. (corresponds to Q1-6)

REFERENCES

[1] N. Gallardo, N. Gamez, P. Rad and M. Jamshidi, "Autonomous decision making for a driver-less car," 2017 12th System of Systems Engineering Conference (SoSE), 2017, pp. 1-6, doi: 10.1109/SYSOSE.2017.7994953.

[2] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898-2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.