Protect Autonomous Vehicles against Cyber attacks with advanced Threat Modeling

Saran Prasad

Individual Student Project Report

Overview

Talking about the overview of our project can only be done using the high level categories that we have identified for analyzing threats and building threat models. The following are the categories that we identified,

1. Ecosystem

This category talks about the various technologies that an AV makes use of like communication protocols, sensors, etc which are used for decision making. This also opens up various attack surfaces. Effective communication protocols, such as Vehicle-to-Vehicle (V2V) using **DSRC** and **Cellular-V2X**, play a pivotal role in enhancing safety and maneuver planning. They heavily rely on sensor fusion, combining data from cameras, **LiDAR**, **RADARs**, and ultrasonic sensors for precise decision-making. The connected automated vehicle (**CAV**) ecosystem operates on a three-tier topology - Cloud servers, fog computing through Roadside Units (RSUs), and edge devices in CAVs. This architecture optimizes real-time data analysis, communication, and overall performance. The reference architecture for CAVs breaks down into Edge, Fog, and Cloud sub-architectures, each serving distinct roles.

2. Threat Modeling and Risk Assessment

Threat modeling strategies are explored. Both generalized and specific ones for AVs have been studied. Focusing on their assets, types of threats, threat modeling frameworks and technologies/frameworks. It gives weightage to the Ecosystem components discussed prior. Exploring attack entry points like physical access, sensors, deep learning models, and roadside signs. Additionally, we discuss various threats, including **OBD** threats, **DSRC** security issues, malware attacks, and threats related to automobile apps. We delve into threat modeling processes such as the **STRIDE** threat modeling process and the STRIDE-based **TARA** framework. It further introduces integrated approaches to AV threat modeling, comparing standards like **ISO/SAE 21434** and **STPA-SEC**, and proposing a novel threat modeling

approach for AVs. Lastly, it explores threat modeling with the Auto Security Development Framework (ASDF) and introduces a risk assessment framework called **SINADRA** for automotive cybersecurity.

3. Attack Analysis
A study has been completed regarding the various attack vectors on AVs. Key vulnerabilities are identified across automotive control systems, autonomous-driving components, and V2X communication technologies. The study categorizes attacks into **passive** and **active** types, encompassing intentional (malicious actors) and unintentional threats (machine learning biases). Specific threats include sensor jamming, **DoS** attacks, information disclosure, and adversarial machine learning. Attack scenarios cover vectors like sensors, communication interfaces, and location tracking. Existing solutions encompass traditional rule-based and AI-based approaches. Overall, the study underscores the importance of robust security measures, continuous monitoring, and countermeasures to ensure the safety and reliability of autonomous vehicles.

4. Threat Mitigation
This category delves into the multifaceted landscape of security and privacy considerations in autonomous vehicles (AVs). Traffic flow optimization, platooning, carpooling, parking systems, Internet of Vehicles (IoV), and Autonomous Vehicles Cloud Computing (AVCC) are scrutinized. Also, with proposed solutions ranging from encryption to blockchain-enabled security. A meticulous exploration of spoofing attacks, notably **GPS** and **LiDAR** replay attacks, is presented. The Extended Kalman Filter (**EKF**) Reconfiguration Scheme is spotlighted for its role in adaptively selecting sensor measurements based on real-time cyber-attack assessments, ensuring accurate vehicle pose estimation. Noteworthy experiments conducted on an Autoware and Gazebo simulation platform underscore the scheme's efficacy. The study concludes with an insightful discussion on safety standards, emphasizing **ISO 26262**, **SAE J3061**, and the British Standards Institute's Cyber Security Standard, collectively fostering a robust and secure approach to the development and deployment of connected and autonomous vehicles.

Contributions

Primary contribution to the project included studies under "**Ecosystem**" and "**Threat Mitigation**" categories. A total of **5 in-depth studies** have been completed which immensely added value to the entire project outcome. The details of these are as follows,

Study 1 - Vehicle-to-Vehicle Communication for Autonomous Vehicles: Safety and Maneuver Planning
This study centers on the communication protocols used by Autonomous Vehicles (AVs), particularly Vehicle-to-Vehicle (V2V) communication. The study also focuses on Dedicated Short-Range Communications (DSRC) and Cellular-V2X (C-V2X) technologies, highlighting their role in addressing safety concerns and maneuver planning, emphasizing the limited broadcast radius of these protocols for inter-vehicle communication. Additionally, it explores the cybersecurity risks, underscoring the potential leakage of critical AV information and the consequential threat of inducing unsafe corrective actions through cyberattacks.

Study 2 - Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models
This study investigates threats to Autonomous Vehicles' (AVs) decision-making and learning algorithms for the creation of the STRIDE threat model. The study also underscores that, even without compromising internal networks or communication protocols, AV decision-making is susceptible to manipulation through smart techniques exploiting Machine Learning (ML) and Deep Learning (DL) algorithm vulnerabilities. It classifies threats into Intentional (malicious actors exploiting AI weaknesses) and

Unintentional (biases or limitations in ML techniques) categories. The identified attacks, such as Sensor Jamming and Denial of Service, pose risks to AV systems, affecting communication protocols like V2I, V2V, V2G, V2C, and V2X. The study also delves into Adversarial ML, illustrating instances where attackers deceive AV systems, impacting crucial control dynamics like steering, perception, and speed regulation.

Study 3 - DARTS: Deceiving Autonomous Cars with Toxic Signs

This study represents a pivotal phase in our project, focusing explicitly on a specific type of attack to inform the STRIDE threat model and risk assessment templates. Outlining key categories, including new attack vectors such as creating deceptive traffic signs and logos that appear normal to humans but trigger malicious responses in AVs' computer vision algorithms. The experimental analysis encompasses scenarios tested in both virtual and real environments, involving two types of adversaries: White box (with detailed system knowledge) and Black box (limited knowledge). It also addresses mitigation strategies, contributing significantly to the project's outcome of Threat Mitigation. The technical attack pipeline involves steps like choosing input, generating robust adversarial examples, and testing in real-world conditions. Lenticular printing attacks, explored in detail, leverage the angle at which signs are viewed, revealing insights into AV misinterpretations based on viewing angles. These findings contribute valuable insights to the broader understanding of adversarial attacks in AV systems.

Study 4 - An Integrated Approach of Threat Analysis for Autonomous Vehicles Perception System

This study addresses the essential question of "**What areas to focus on when developing threat frameworks for AVs.**" It introduces a novel TARA framework, integrating insights from studies conducted on AV technologies and cybersecurity standards such as **ISO/SAE 21434** and **STPA-SEC**. Emphasizing the commonalities between these standards, highlighting sequential steps and strategies for threat identification, risk assessment, and mitigation. The integrated framework prioritizes analyzing AV perception systems as complex cyber-physical systems, evaluating AI algorithm robustness, assessing attack potential, and considering mitigation factors. Notably, it introduces mathematical factors like **MUSecX** and **RUSecX** to quantify the overall risk by combining potential damage severity, attack feasibility, and mitigation effectiveness. This approach provides a comprehensive and nuanced threat analysis and risk assessment framework for AV perception systems, considering the dynamic environment, and AI algorithm vulnerabilities in autonomous vehicles.

Study 5 - Autoinfotainment Security Development Framework (ASDF) for Smart Cars

This study focuses on securing Autonomous Vehicles (AVs) by reviewing and developing frameworks for specific technologies. It explores the Controller Area Network Bus (CAN Bus) as a unique protocol for distributed control systems and addresses vulnerabilities in Smarter Vehicles Cyber Security, including potential threats to systems like DSRC. The Auto Information Development Framework (AIDF) is introduced for smart AVs, with layers like **End Users**, **Communication**, **Services**, and **Applications**. To counter vulnerabilities within the AIDF framework, the paper presents the **Auto Security Development Framework** (ASDF), featuring a 2D architecture with layers and planes. Advanced intrusion detection systems, such as **Multi-Level IDS** (MLIDS) and **Anomaly Behavior Analysis** (ABA) Methodology, are introduced using machine learning techniques. Experimental results validate the proposed security frameworks, showcasing robust performance even under challenging scenarios like frame drops, interference, and wireless channel issues. The paper provides a concise yet comprehensive exploration of tailored security frameworks for specific AV technologies, supported by practical experiments that affirm the efficacy of the proposed approaches.

As the **deputy leader**, important tasks such as meeting scheduling, assigning papers and categories to group members, etc were performed. This also includes peer review of in-depth reports, giving feedback, setting goals for each week and resolving open issues within the group. Significant contribution to the

initial **project scope and outcomes** was done, continuing the efforts throughout the project timeline in refining and solidifying **final deliverables**. Another important contribution would be the extensive collection of research papers that are relevant to the topic. This contributed to broadening the project's scope and enhancing its outcomes, resulting in an overall more robust project.

Lessons Learned

A lot of technical as well non-technical lessons have been learned throughout the semester while doing the project.

1. Technical Aspects

Although our project initially centered around security, it became evident that a comprehensive understanding of all aspects of **Autonomous Vehicles** (AVs) is essential to address security effectively. To structure our studies, we identified **high-level categories**, ranging from analyzing AV technologies to studying threat analysis frameworks. This approach facilitated a holistic comprehension of AVs and their underlying technologies, offering an **end-to-end perspective**.

My primary responsibility, delving into attack vectors, led me to explore **Machine Learning (ML) and Deep Learning (DL)** extensively. Numerous attack vectors exploited biases in contemporary DL algorithms, prompting me to delve into **cutting-edge DL technologies** and their applications in AVs. This exploration illuminated the dynamic nature of an "arms race," particularly in the realm of Artificial Intelligence (AI).

Beyond enhancing my expertise in familiar domains, I had the opportunity to explore new concepts, particularly in **communication, threat analysis, and the development of threat frameworks**. Recognizing the pivotal role of international standards in shaping the AV industry, I discovered that there is no universal solution applicable to all challenges. The intricate landscape of AVs demands tailored and adaptive approaches to problem-solving in today's evolving environment.

2. Non-technical aspects

Taking on the role of deputy leader within the group provided me with invaluable experience in **team coordination** and honed my **managerial skills**. Engaging in tasks such as assigning responsibilities, scheduling meetings, offering constructive feedback, and assisting group members enhanced my understanding of effective leadership. This experience not only shed light on my **strengths and weaknesses** as a leader but also illuminated areas for improvement in my future endeavors.

In addition to leadership insights, being in a leadership position equipped me with a deeper understanding of effective **group dynamics**. Recognizing the leader's perspective in focusing on the **bigger picture** while delegating tasks to individual members enhanced my ability to contribute meaningfully to group objectives.

Beyond positively influencing team synergy and coordination, the project demanded a significant investment of time and effort, prompting me to refine my time management skills. Balancing multiple responsibilities required careful planning and execution, fostering an improved ability to allocate my time effectively. Moreover, as efficient project execution relied on a thorough understanding of relevant literature, I developed the skill of **reading papers more efficiently**. This experience empowered me to devise **quicker strategies** for comprehending research papers without getting bogged down in minute details. Overall, my role as deputy leader not only contributed to the success of the project but also provided a platform for **personal and professional growth**.

References

[1] M. Girdhar, J. Hong and J. Moore, "Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 417-437, 2023, doi: 10.1109/OJVT.2023.3265363.

[2] A. Ali, L. Jiang, S. Patil, J. Li and R. W. Heath, "Vehicle-to-Vehicle Communication for Autonomous Vehicles: Safety and Maneuver Planning," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-5, doi: 10.1109/VTCFall.2018.8690946.

[3] S. Ghosh, A. Zaboli, J. Hong, and J. Kwon, “An integrated approach of threat analysis for autonomous vehicles perception system,” IEEE Access, vol. 11, pp. 14752–14777, 2023

[4] P. Satam, J. Pacheco, S. Hariri and M. Horani, "Autoinfotainment Security Development Framework (ASDF) for Smart Cars," 2017 International Conference on Cloud and Autonomic Computing (ICCAC), Tucson, AZ, USA, 2017, pp. 153-159, doi: 10.1109/ICCAC.2017.22.

[5] Chawin Sitawarin, Arjun Nitin Bhagoji, Arsalan Mosenia, Mung Chiang, Prateek Mittal, “DARTS: Deceiving Autonomous Cars with Toxic Signs” in “ACM CCS 2018”, 2018, Toronto, Canada