Final Report

Catalyst Fellowship Program

AJ Khan

Founder & CEO, Vehiqilla Inc.

Dated: September 13, 2023

Contents

Introduction

AJ Khan joined the Rogers Cybersecure Catalyst Fellowship Program to further Vehiqilla Inc.'s research in Connected & Autonomous Vehicles (CAVs). This research aimed to verify two central questions regarding the development of CAVs. First, CAVs do not follow Secure Software Development Life Cycle (Secure SDLC) best practices and thus, can be easily hacked. Second, CAVs need to have real-time cyber monitoring to ensure that any security event is identified so that appropriate measures taken to mitigate the impact of this cyber event.

The development of CAVs has changed our transportation roadmap. The modern vehicle is equipped with 100's of Electronic Control Units (ECUs) that together contain many million lines of code. Due to this connectivity, a vehicle can communicate not only with systems in the Cloud through the Internet, but also with other vehicles and with roadside infrastructure such as traffic signals. Access to any one of these might enable data leakage or provide control of the vehicle to unauthorized parties. This makes CAVs susceptible to cyber risks including invasion of Privacy, Connection Risks, Mobile Application Vulnerabilities, Supply Chain Cybersecurity Vulnerabilities, Manipulation of safety critical control, and Vehicle theft.

To further the initiative with the Rogers Cybersecure Catalyst, the research was structured in two separate phases, each with distinct focus on tools and techniques to build the related problem solution :

- Phase 1: Penetration Testing Methodologies for CAVs
    - Understanding CAV Architecture
    - Identify Attack Vectors to attack a CAV
    - Analyzing hacking tools and methodologies that might be used to hack into a CAV
- Phase 2: Incident Management for CAVs
    - Develop a lab on AWS to validate MVP solution of Vehiqilla VSOC
    - Research Technical solutions related to deploying VSOCs.
    - Enable real-time cyber monitoring by sending CANbus messages to Vehiqilla VSOC

The Catalyst Fellowship Program has enabled this research in many significant aspects. This includes:

- Interaction with other Industry & Academic Researchers that are part of the Catalyst Fellowship Program.
- Participation in enabling webinars & white papers related to cybersecurity topics.
- Engagement with Rogers CyberSecure Catalyst Executive team.
- Focus on research with cyber intern.
- Providing opportunities to further this discussion in the cyber ecosystem of Canada.

Review of the Bibliography

AJ Khan has worked extensively in the field of Automotive Cybersecurity. He is currently the President of the Global Syndicate for Mobility Cybersecurity (GSMC), a not-for-profit entity which focuses on ensuring cybersecurity is built into all forms of Mobility. He is also the founder & CEO of Vehiqilla Inc., an automotive cybersecurity startup focused on providing real-time cyber monitoring of Vehicles through its VSOCs. AJ has been deeply involved in various automotive cybersecurity initiatives in recent years. From January 2019 to February 2021, he was the co-chair of the Cyber Security Committee of the Automotive Parts Manufacturers Association (APMA) of Canada. He has also contributed to CAV initiatives by Transport Canada and European Union Information Security Agency (ENISA). AJ has been repeatedly recognized for his work and was awarded the prestigious Donald S. Wood Leadership award by APMA in 2021 for his leadership in the field of automotive cybersecurity.

AJ has also written a book, "Automotive Cyber Governance" on Automotive Cybersecurity. In this book, AJ has emphasized the need to build a Cyber Mindset to ensure that the cyber challenges in the automotive sector are adequately addressed. This Cyber Mindset begins by comprehending the impact of cyber threats to the Vehicle of the Future and why these cyber threats threaten the health & safety of the passengers of these vehicles. AJ highlights that by encompassing Cyber Governance, Risk & Compliance and Security by Design, Cyber Risk in Connected & Autonomous Vehicles (CAVs) can be significantly mitigated. The crux of this book is all about the development and execution of a holistic cybersecurity strategy for any automotive organization. This detailed Cyber Strategy must be accompanied by a comprehensive roadmap that encompasses all aspects of this strategy. AJ has also highlighted the Cyber standards and mandates that are specific to the automotive sector. These include the recently published ISO 21434 Road Vehicles Cybersecurity Engineering Standard as well as the UNECE WP.29 R155 & R156. Finally, AJ outlines other key cybersecurity practices including Risk Assessment, Cyber Supply Chain Risk Management (C-SCRM), Operations Cybersecurity and of course, Human beings as the weakest link.

Furthermore, AJ is a recognized thought leader in this space and has spoken extensively on Automotive Cybersecurity on various forums.

Methods & Materials

There have been three critical areas of activities that I have been involved in during the Rogers Cybersecure Catalyst Fellowship program. These include:

- Webinars
  - Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research
  - The Hunt for Hack-Tastic Talent: Analyzing the Cyber Talent Shortage
  - Developing a Successful Cyber IP Commercialization Strategy
- Position Papers
  - Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research
  - Bridging the Cybersecurity Talent Gap:
    Training Talent and Cultivating a Strong Cybersecurity Culture
  - Pathways on Developing a Successful Cybersecurity IP Commercialization Strategy
- Working with Interns to further Automotive Cybersecurity Research
  - Phase 1: Penetration Testing Methodologies for CAVs
  - Phase 2: Incident Management for CAVs

The combined expertise and experience of the Fellows that are part of the Catalyst Followship program has created a wealth of knowledge for the wider cybersecurity community. The webinars that have been organized have provided useful thought leadership on various cyber challenges such as the first webinar on enabling collaboration between Academia & Industry in Cybersecurity Research. The next webinars also broke new ground in highlighting challenges in meeting the cybersecurity talent gap. The final webinar on developing a successful cyber IP commercialization was very well received by the wider cybersecurity community, and is being lauded as a major source of knowledge for the advancement of IP strategy of many cyber startups and scaleups in the Canadian cyber community.

A highlight of the program has been the position papers written by the fellows. The process of co-authoring papers around these complex cyber questions has brought together a very insightful discussion on addressing all these three areas of cyber research. These papers have been well received in the industry, and the fact that they are being accepted for publication itself highlights the success of the Catalyst Fellowship program in enabling these discussions.

The final activity that has been part of this fellowship is the research carried out with the Interns on Automotive Cybersecurity. This research has validated Vehiqilla's approach towards enhancing the cybersecurity of CAVs. The outcome of the first phase of research was a comprehensive white paper Ethical Hacking of CAVs that defines detailed tools & methodologies for carrying out such Ethical Hacking. The second phase of the research validated the MVP of Vehiqilla VSOC by establishing the environment in AWS and enabling the detection of Indicators of Compromise (IoCs) from CANbus messages.

Results & Discussions

The Rogers Cybersecure Catalyst's Catalyst Fellowship Program has achieved its aim to foster more collaboration between Academic and Industry Researchers. The webinars produced and the position papers co-authored are great examples of this collaboration. These webinars and position papers provides a unique perspective as it brings together the Catalyst Fellowship Program's Academic and Industry Researchers to develop a conversation around cybersecurity challenges that our society is currently facing. This thought leadership has provided insightful and detailed knowledge for further cyber research that can be used to develop new areas of cybersecurity.

Another success of this program has been the research enabled between myself as the researcher and the Interns associated with me. This research has provided a playbook for carrying out Ethical Hacking on a Connected & Autonomous Vehicle (CAVs), and also validated the MVP of Vehiqilla Inc. This means that Vehiqilla can further its defined goal of ensuring automotive cybersecurity and make our roads safer.

Recommendations

Below are some of the recommendations to further the aims of the Catalyst Fellowship Program

- Rogers Cybersecure Catalyst should have its own publication to publish research papers.
- Opportunities to interact with international research organizations should be enabled.
- Webinar production quality needs to be enhanced.
- More avenues for collaboration opportunity between researchers and Cybersecure Catalyst needs to be enabled.
- Funding opportunities for researchers should be enabled by Cybersecure Catalyst.

Bibliography

[1] KPMG APMA Canadian Automotive Cyber Preparedness Report February 2021. (https://apma.ca/2021/02/17/canadian-automotive-cyber-preparedness-report/)

[2] ISO/SAE 21434:2021 Road Vehicles Cybersecurity Engineering. (https://www.iso.org/standard/70918.html)

[3] UNECE WP.29 R155:Cybersecurity and Cybersecurity Management System (https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security)

[4] UNECE WP.29 R156: Software Update and Software Update Management System (https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update)

[5] CSA Group: Working Group on CAV Cybersecurity, Privacy & Data Management

[6] AJ Khan “Automotive Cyber Governance: Opportunities & Challenges for Cybersecurity in Connected & Autonomous Vehicles (CAVs)” Amazon 2022

[7] Webinar: Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research

[8] Position Paper: Bridging the Bubbles: Connecting Academia and Industry in Cybersecurity Research