Texas A&M Transportation Institute
3135 TAMU
College Station, TX 77843-3135

979-317-2863
http://tti.tamu.edu

MEETING NOTES

TxDOT IAC – Technical Support to the CAV Task Force

DATE: July 6, 2024

TO: Zeke Reyna, Emerging Technology Team Lead, STR, TxDOT
Lauren Freriks, Strategic Management Analyst, STR, TxDOT

COPY TO: Beverly Storey, Research Scientist, TTI
TTI_Reports@tti.tamu.edu
Tim Hein, Research Development Office, TTI

FROM: Robert Brydia, Research Supervisor
Senior Research Scientist, Texas A&M Transportation Institute

RE: Data, Connectivity, Cyber Security and Privacy Subcommittee
June 21, 2024, Meeting Notes

Attendees:

Adrian Pearmine	STV
Alex Aragon	Office of the Governor of Texas
Austin Holder	Office of the Governor of Texas
Bob Brydia	Texas A&M Transportation Institute
Brian Steiner	Cisco
Cliff Heise	Iteris
Daniel Sullivan	Navistar
James Hubbard	Texas A&M Transportation Institute
James Kuhr	STV
Jeffrey Decoux	ATRIUS Industries
Reza Langari	Texas A&M University
Sly Majid	Volkswagen Group of America
Zeke Reyna	Texas Department of Transportation

I. Welcome and Introductions - Zeke Reyna, TxDOT

- Thank you for joining this Data subcommittee of the Texas CAV Task Force
- We are looking forward to what we can accomplish together

II. Opening Comments - Subcommittee Chair: Brian Steiner, Cisco

- Thank you for joining this meeting
- We appreciate your participation and feedback

III. Priority Topics Presentation

- Data Priority Topics
  - Where do the cybersecurity risks lie?
  - How are customers/users being protected?
- Upcoming Efforts
  - Interview more industry participants (we need you!)
  - Finalize risk categories
  - White paper annotated outline
  - Annotated outline feedback
  - White paper draft
- Risk Categories
  - CAVs Penetration
    - Expanded attack surface due to numerous connected systems
    - Legacy system vulnerabilities from outdated infrastructure
    - Varied attack vectors targeting different communication protocols (V2V, V2I)
    - Complexity of systems means any vulnerability can be exploited
    - Interconnectedness allows attacks to spread across the network
    - Need for robust, multi-layered security solutions to address complex threats.
  - CAVs Communication Framework
    - Interoperability issues due to lack of standardization across manufacturers
    - Data privacy concerns related to personal information exchange
    - Necessity for real-time threat detection using advanced technologies (AI, ML)
    - Importance of industry collaboration to establish secure communication standards
    - Encryption, anonymization, and secure data storage to protect user privacy (Data exchanges)
    - Regular audits to ensure compliance with privacy regulations and standards
  - Secured CAVs Proximity Access
    - Advanced authentication methods (multi-factor, biometrics, rolling codes)
    - Signal encryption and jamming to address emerging vulnerabilities
    - User education on proper use and importance of security features
    - Integration of physical and digital security measures for comprehensive protection
    - Rapid detection and response mechanisms to minimize damage from breaches.
    - Public will most likely “see” news information the most about a breach or security issue

        - Human to device communication
    - Human CAVs Cyber-Safety Awareness
        - User education programs covering cybersecurity risks and best practices
        - Mitigating human error through continuous training and user-friendly security features
        - Tailored training programs for different user groups (owners, fleet operators, maintenance)
        - Proactive approach to user education to prevent cyber incidents
        - Ongoing education and training to keep users informed about evolving threats
        - Scenario-based training exercises to prepare for potential security incidents
    - Regulatory Laws and Policy Framework
        - Standardize on public sector side
        - Expectations
    - Building trust across the industry (OEMs) and among the public
        - Transparent communication about security practices and incident response
        - Collaborative threat intelligence sharing among OEMs to enhance overall security
        - Public awareness initiatives to educate consumers and address concerns
        - Proactive and transparent handling of security breaches to maintain trust
        - Fostering a culture of security awareness to encourage adoption of CAV technology
        - Engaging with consumers through educational initiatives and public outreach programs.
- Future Opportunities
    - Unified cybersecurity standards across regions and manufacturers
    - Compliance monitoring and enforcement through audits and penalties
    - Adaptable legislation to keep pace with technological advancements
    - Collaboration among regulatory bodies, industry, and experts to develop effective policies
    - Providing support and guidance to manufacturers to navigate the regulatory landscape
    - Fostering a culture of compliance within the industry to prioritize cybersecurity

IV. Next Steps

- If any members are willing to allow us to reach out to you for a 20 to 30-minute conversation about one or two of these big picture questions, ensuring that we understand your concerns from the angle of the industry, we would love that opportunity.
- Please don't hesitate to reach out to us with questions and/or comments

V. Closing Remarks – Zeke Reyna, TxDOT

- We are excited to see how this white paper develops and look forward to your input
- This has been a great commentary feedback and we really appreciate your ongoing participation

VI. Adjourn