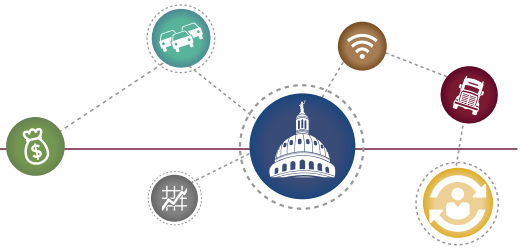
Texas A&M Transportation Institute

Revolutionizing our Roadways

Cybersecurity Considerations for Connected and Automated Vehicle Policy



TRANSPORTATION
Policy Research CENTER

Revolutionizing our Roadways

Cybersecurity Considerations for Connected and Automated Vehicle Policy

by

Dominie Garcia, Ph.D
Booz/Allen/Hamilton

Chris Hill, Ph.D.
Booz/Allen/Hamilton

Jason Wagner
Texas A&M Transportation Institute

Texas A&M Transportation Institute
The Texas A&M University System
College Station, Texas 77843-3135

Published: January 2015

CONTENTS

Introduction

Relevant Types of Security

As connected and automated vehicle technologies advance, national and state legislators and policy makers must address the need for policy, guidance, standards, regulations, and other frameworks for ensuring that these technologies are implemented in a secure environment.

Security for automated and connected vehicle technologies involves two broad categories, both of which are relevant and of interest to legislators, and can be defined as follows:

- **In-vehicle security** – what exists to guard against tampering with electronic and computerized systems, either from within or from an external source communicating with a vehicle. As automobile manufacturers develop more options for connectivity, such as 4G capabilities, the opportunities for breaching in-vehicle security increase.
- **"Cyber" security** – in the context of vehicle systems, this refers to security protections for systems in the vehicle that actively communicate with other systems or other vehicles.

In-vehicle security work has thus far been the less attended of the two areas. Recent attention to in-vehicle security is increasing, as the potential risks and threats to vehicle systems increase based on advancing technology. The few efforts that the authors are aware of in this area are being led by the automobile manufacturers, and the results of those efforts have not been shared publicly. Nonetheless, as vehicles become more connected through various media and the numbers of internal systems increase the possibilities for attack, we expect more attention to be focused on in-vehicle security issues.

Recent attention to in-vehicle security is increasing, as the potential risks and threats to vehicle systems increase based on advancing technology.

To date, much of the work on security for connected vehicles (in the "cyber" security realm) has been led by the United States Department of Transportation (USDOT) as background and input for the National Highway Traffic Safety Administration (NHTSA) decision about potential regulation of connected vehicle technology for safety applications. The USDOT has also sponsored a number of research and development projects around non-safety applications, though security systems for these have not yet been designed. Security for infrastructure and non-safety applications, those of great interest to states, have not yet been addressed by the USDOT-led research, thus presenting a number of open opportunities for states and their partners to research and develop security designs and policies in these contexts.

Federal Security Guidance

It is envisioned that any security aspects related to infrastructure components will be promulgated by the Federal Highway Administration (FHWA) in the form of guidance, rather than in the form of regulation, to be released by 2015. There may be additional requirements or specifications/standards attached to federal-aid funding for infrastructure elements. The nature of such guidelines has not been specified, though the USDOT has indicated in public comments that they will be focused on providing implementers with both technical and policy suggestions and guiding principles to help with implementation planning and operation of infrastructure and back end systems to support connected vehicle applications. FHWA has suggested that guidance areas may include use of right-of-way, innovative financing, interoperability, and interaction with federal aid processes. Other guidance products may also be required to cover areas such as cybersecurity, benefit-cost analyses, and systems engineering processes. As this research and analysis are in the early stages, states can be active participants and influence the process of developing and standardizing these aspects of security for connected and automated vehicle infrastructure and operations.

Comparing Security for Connected and Automated Vehicle Technology

Connected and automated vehicles are closely related, though there are distinct areas of current research and future deployment. Robust security systems are required for both, and the needs of those systems are anticipated to be different in many aspects. Several researchers maintain that many of the aspects of connected vehicles, both in terms of security and operations/applications, will be applicable to automated vehicles, especially in the context of communications and connectivity with other systems. This paper addresses many of those differences and similarities throughout, with explicit discussion of when we see comparability or differences between connected and automated vehicles.

As this research and analysis are in the early stages, states can be active participants and influence the process of developing and standardizing these aspects of security.

Focus of this Report

In this report, we outline a set of high-level questions that should guide the research and analysis, as well as future development of state-level policies or regulations. Before state legislators undertake the tasks of setting policies, they must first understand what these two types of security (in-vehicle and cyber) imply and what the needs are based on the technologies and envisioned implementations of connected and automated vehicles. The implications of the two types of security protections vary based on technical designs and who is responsible for the implementation and management of those systems. At this point, much of the in-vehicle security that is being researched is envisioned to be under the purview of the automobile manufacturers, though as those solutions apply to technologies that

are related to connected vehicle applications and systems, there may be additional policy implications that states must consider. This paper focuses on cyber security research and the related policy implications and considerations for state regulators.

For each set of questions, we provide a summary of current thinking and research, as well as implications and considerations for state law makers. We also make recommendations throughout about how states can approach these areas and sets of questions in order to gain both a comprehensive understanding of the need for various levels of state oversight on security and to develop a set of policies that can help ensure protection of their citizens.

One important note: although we include discussion of both connected and automated vehicles, many of the policy implications for the latter will be (at least in part) determined or influenced by, or the same as the former when it comes to security. This paper does not look at the elements related to application operations[1] that states may want to regulate or oversee. Rather, the paper is focused on specific security issues shown here.

Role of Technical Designs

Although there is a difference between technical designs of the connected and automated vehicle systems and technical design for the security, several aspects of the overall technical designs are driven by the need for certain security protections. For example, the data elements included in certain messages, such as the Basic Safety Message for vehicle to vehicle (V2V) communications, have been defined so as to provide "privacy by design." Furthermore, the technical design of the security systems will be driven by the technical designs and specifications of the applications. Although this report is focused on the design and policy implications of the security system(s), the implications both to and from the technical designs of the underlying system are interrelated and therefore are referred to when relevant.

[1]The concept of "applications" (and thus their operations) in the connected vehicle environment refers to programs that are designed to operate on the connected vehicle device within a vehicle and provide different services to the driver, such as safety warnings, information about the environment or congestion, or notices from the infrastructure, among many others.

Safety applications are those that help drivers attend to crash imminent situations, such as blind-spot warnings or curve speed warnings.

Security versus Safety

There is an additional note of clarification about security versus safety, concepts often confounded. Safety applications are those that help drivers attend to crash imminent situations, such as blind-spot warnings or curve speed warnings. Security relates specifically to the back end, underlying system that ensures that users within the system are trusted and trustable and that messages maintain integrity, authenticity, and confidentiality when required based on the information being transmitted. This report is focused on security of the envisioned connected and automated vehicle systems.

Security

As state, regional, and local jurisdictions consider planning for implementation of various connected and automated vehicle system elements, it is paramount that they begin with an understanding of the technical requirements and designs necessary for ensuring the security of users and their data. Coupling the technical needs and designs with the specific policy environments will help lawmakers and regulators develop their own policy frameworks.

Policy environments vary from state to state and even from region to region. Beyond whatever federal guidance or regulations are released, each state or region will have to develop its own principles, guidance, and/or regulations according to its particular needs, goals, and policy framework. Clearly, policy and legislation cannot be developed in contradiction to technical designs and requirements, but rather the technical designs should support policy requirements, and vice versa. In this section, we include the basic elements of security designs and requirements for both connected and automated vehicle systems, in so far as they exist, and relate those technical elements back to policy considerations at the state level.

There is no preset requirement for states to develop additional levels of security, beyond what the federal regulations imply or what commercial or private organizations implement. Nonetheless, because states have distinct privacy and security approaches or goals, one can reasonably expect that some states may choose to enact additional security regulations or guidelines with which they could require connected vehicle organizations to comply. Consideration of both a state's perspective and goals related to security, as well as the impact on existing state systems and technologies, will also influence the decision-making process as states consider whether to expand on the federal guidance or commercial security designs. The box below includes the high level questions that will guide this discussion.

Security Issues Focus of this Paper

How to ensure:

- **Data integrity and accuracy.[2]**
- **Data is not used inappropriately.**
- **Users in the system are authorized or trustable.**
- **Hacking or malfeasance related to behavior within the system is protected against.**

How to provide a system-wide security structure that protects all users and operators from a wide range of threats and risks.

[2]Security system design consistently includes consideration of data integrity and accuracy. The security system must protect not only access to data but ensure that transmitted data maintains its integrity during transmission to ensure that the system is trustable.
[3]http://www.its.dot.gov/connected_vehicle/principles_connectedvehicle_environment.htm, last accessed: April 4, 2014

Guiding Questions for Security Discussion

1. What is the current design for the security system (e.g., Public Key Infrastructure for V2V Safety messages)?
2. Will AV security system(s) be based on the same principles as CV security?
3. What are additional needs for AV that may imply the need for different security systems than for CV?
4. How do the technical designs inform the development of federal, and state, and local policy needs?
5. What are the standards and levels of security that will be guaranteed by the system?
6. What will states and local agencies be responsible for in terms of operating, maintaining, or owning elements of the security system? (infrastructure, certificate management entities, oversight and management, etc.)
7. How can states provide additional levels of security protection to their users?
8. How do states manage and integrate new security systems with their existing infrastructure?

Security Systems – Questions 1 through 5

Much of the work done to date on developing security systems for the future connected vehicle system has been sponsored by the USDOT in an effort to explore how a system can be designed to ensure several national priorities for security and privacy. The USDOT has developed a set of principles that can be thought of as "goals" for system design. The current security system design for V2V safety communications complies with the principles. They are broad in their scope and open to interpretation and design or policy choices for compliance. USDOT has indicated that the principles should be used as guidance in developing implementation plans, rather than steadfast rules that have to be followed to the letter. They are described as follows[3]:

Principles/Goals for Security System Design

Purpose

- Transportation safety is the DOT's top priority for the connected vehicle environment. The system must:
  - Prevent or mitigate the severity of crashes
  - Minimize driver workload
  - Ensure no increase to driver distraction
  - Encompass all road users
  - Ensure that mandatory safety applications cannot be turned off or overridden.
- Uses beyond safety applications, especially for mobility and environmental purposes, are permissible and encouraged as long as they do not detract from safety.

Coverage/Scale

- The system is applicable to all types of connected vehicle systems and applications (safety, mobility, environmental, etc.).
- System implementation must be national in scale and extensible across North America.

User Protections

- DOT is committed to fostering a connected vehicle environment that ensures stakeholder and operational needs are met while at the same time protecting consumers appropriately from unwarranted privacy risks.
  - The connected vehicle environment will incorporate appropriate privacy controls: transparency; individual participation and redress; purpose specification; limitations on use of information; data minimization and retention; data quality and integrity; security; and accountability and auditing. For example:
- The environment must provide consumers with appropriate advance notice of and, for opt-in systems[4], opportunity to provide consent for information collection, use, access, maintenance, security and disposal.

[4]The term "opt-in" is a general one used to indicate any optional service or program/application, regardless of how that program is operated; i.e., it could be envisioned as "opt-out." The distinction being drawn is one of mandated versus voluntary participation.

- The environment will limit the collection and retention of personally identifiable information to the minimum necessary to support stakeholder and operational needs[5].
  - As the federal role and other critical aspects of connected vehicle regulation and/or implementation are further defined, DOT will document publicly the privacy risks and controls applicable to the system and users.
- The system must be secure to an appropriate level. The system will:
  - Ensure secure and trusted information exchange among users
  - Provide protection from hacking and malicious behavior
  - Maintain data integrity.

Implementation and Oversight

- An organization will be required to manage and operate the system responsible for ensuring security and other functions associated with the proper operation of the connected vehicle system.
  - This organization can be private, public or a private/public hybrid.
  - This organization will be governed by rules and methods of operations that ensure compliance with DOT connected vehicle principles and any other rules or requirements that may be established by the DOT with input by stakeholders.
  - All key parties will have a voice.[6]
- Consideration should be given to allow applications from sources outside the governance structure on to the system, as long as they are in compliance with all established system principles, including security and operational requirements.
- The system should be implemented to provide ongoing operations.
  - If state and local agencies are involved in system implementation, the system should be designed to be cost beneficial for state and local transportation agencies in regards to building, operating, and maintaining.
  - USDOT is receptive to all sustainable financing options that do not violate other Principles. In the event that that the only viable financing option relies on financing from participating organizations, companies, or entities, the common operating costs for the system including security, governance and other costs should, to the extent feasible, be shared.
- There can be no consumer subscription fees for mandatory safety applications.
  - Does not preclude mandatory universally applicable taxes or fees to finance the system[7]
  - Subscription or other fees for non-mandatory, opt-in applications are possible.

Technical Functionality

- Functionality of the system requires compliance with nationwide, universally accepted, non-proprietary communication and performance standards.
  - Interoperability of equipment, vehicles, and other devices is necessary to enable mandatory safety applications as well as applications supporting mobility, economic competitiveness, and sustainability.
  - Standards must be maintained to ensure technical viability.
- The system must be technically adaptable and viable over time.
  - It must be backward compatible
  - The system must be able to evolve over time as new technologies become available.
- Communication technology for safety applications must be secure, low latency, mature, stable, and work at highway speeds.
  - Currently DSRC is the only known viable technology for safety critical applications.
  - DSRC or other communication technologies could be used for safety applications that are not for

[5]The most recent published work on this topic was completed in 2007 and is described in "Vehicle Infrastructure Integration Privacy Policies Framework, Version 1.0.2," National VII Coalition, February 16, 2007.

[6]Work to define the "key parties" is ongoing. However, initial presentations on a security credentials management system (SCMS) management approach by the Vehicle Integrated Infrastructure Consortium (VIIC), a consortium of carmakers undertaking policy analyses for USDOT, suggests that these parties would include the federal government, state governments (probably through AASHTO), and the carmakers themselves.

[7]Subscription fees refer to ongoing fees that a consumer voluntarily chooses to pay for a service. Mandatory universally applicable fees differ in that they are not voluntary and are therefore likely to either be collected by government agencies (such as in conjunction with vehicle registration) or included in the purchase price of the vehicle or equipment.

crash-imminent situations, mobility, and environmental applications.

- Use of the spectrum must comply with established requirements for non-interference.
  - Safety applications take priority over non safety applications.
  - Public sector applications take precedence over commercial applications.

Design of Public Key Infrastructure System

Currently, one technical design exists to support a national connected vehicle system – a Public Key Infrastructure system to provide security for V2V safety applications. The design is close to finalized, in theory, but elements of it are still under development by the Crash Avoidance Metrics Partnership (CAMP). It has yet to be prototyped or tested, but plans are underway to build prototypes and include the conceptual design in testbeds and pilots in the near future. From August 2012 to August 2013, the Safety Pilot Model Deployment, sponsored by the USDOT and operated by the University of Michigan Transportation Research Institute, along with other contractors and researchers, included a "test SCMS" (Security Credentials Management System). This system, though sharing the same name as the security system design for full deployment, did not follow the current/full design. It was developed only to be used for the Safety Pilot and additional test beds to provide basic levels of digital security for certificates, but was not meant as a prototype or test of the anticipated full security system.

Policy Considerations Related to Technical Design

Researchers and policy experts are exploring the implications of the technical design on various levels of security and policy, examining the need at a national level as well as the needs that private sector organizations may have for taking part in the security system. A broad view of policy considerations that are implied by the needs for security across various connected vehicle applications and scenarios include the following:

- Security Credential Management Operations and Policies
  - Credential Generation and Use
  - Credential Management Functions and Operations
- Unit and Organizational Certification Policies
  - Infrastructure Policies related to the back end security systems, or other elements of the physical and data-based infrastructure that will be needed to support and operate security system(s)
  - Equipment – Hardware, software and laboratory certification policies for on board and roadside equipment
- Misbehavior and Revocation Policies
- Organizational and Operational Expansion/Upgrade Policies
- Privacy Policies: Data Quality, Integrity, Minimization, Retention, Access
- Accountability/Auditing

Currently, one technical design exists to support a national connected vehicle system – a Public Key Infrastructure system to provide security for vehicle to vehicle (V2V) safety applications.

How the technical design for the V2V safety applications can be extended, modified, or added to for various additional applications (i.e., other connected vehicle mobility and environmental applications) is still very much at a nascent stage of research and development. It is not clear whether additional non-safety applications will require their own security systems or be able to operate on the security system designed for safety applications. Nonetheless, USDOT has indicated at this stage that its intention is to regulate only the safety-critical applications, and therefore the security systems that support those applications. The belief is that states will be free to design and implement, or require security outcomes based on their needs and goals, as long as those systems do not interfere with the safety applications and its security and allow for interoperability. This early stage provides state regulators and lawmakers with an opportunity to potentially shape what some of the additional security requirements might be – thus influencing the development of the technical designs of additional security systems for applications that extend beyond V2V safety.

Referring back to the principles set by the USDOT for a national, regulated V2V safety system, states can set their own such principles or requirements, and add on to or leverage the federal principles. If in fact mandated by NHTSA, sates will not be able to change the safety applications portion of the system and will have to comply with the security requirements for safety applications. How the security system will be operated is still under development. At this point, technical and policy experts believe that the security system for V2V safety applications represents the current highest possible level of security.

It is not clear whether additional non-safety applications will require their own security systems or be able to operate on the security system designed for safety applications.

Some of the technical questions that need to be answered about the extensibility, modification, or additional security systems (on top of what has been designed and will be needed for V2V safety applications) include:

- Can the on-board equipment (OBE) support processing and data needs (receipt, storage, sending, etc.) for more than V2V safety applications?
- If the security requirements are less stringent for additional applications, does there need to be a new system in place to support those (e.g., commercial applications that require sending of payment information may not be supportable by the SCMS as currently designed)?[8]
- How are competing applications managed both by the communications networks and the on board technology for prioritization?

As industry technical experts sort through these questions, state policy makers can provide input during the design process to ensure that the security needs that states have for their users and systems are considered or attended to.

Finding: *States should look to develop a set of principles and/or requirements for the levels of security that they want to ensure across multiple applications for both connected and automated vehicles. The principles and requirements should be developed based on a state's missions, vision, goals, and current policies, not based on technical design of any one system or application.*

Considerations of these same questions for future automated vehicle systems and environments are similar. To date, there has been no national or coordinated effort to develop a design for security for automated vehicles. While individual companies may be researching, developing, prototyping, and testing various facets of automation in vehicles, no standards for the technologies exist. In fact, there is no agreement in the transportation sector about what automation truly means. The Society of American Engineers (SAE International) has developed a six-level hierarchy of automation.[9] NHTSA has developed a similar structure, but uses a five-level approach based on the advancement of in-vehicle technology and the applications that a technology supports. We will refer mostly to the NHTSA definitions of automation (included here), though the SAE levels are quite similar.

Hierarchy of Automation

Level 0 – No-Automation. The driver is in complete and sole control of the primary vehicle controls (brake, steering, throttle, and motive power) at all times, and is solely responsible for monitoring the roadway and for safe operation of all vehicle controls. Vehicles that have certain driver support/convenience systems but do not have control authority over steering, braking, or throttle would still be considered "level 0" vehicles.

Level 1 – Function-specific Automation. Automation at this level involves one or more specific control functions; if multiple functions are automated, they operate independently from each other. The driver has overall control, and is solely responsible for safe operation, but

[8]An interesting point related to this is that many people are used to thinking about online financial transactions requiring the highest levels of protection. However, when we move to the vehicle environment, security requirements for safety applications focused on the protection of life in crash-imminent situations are more stringent than security requirements in other situations – including protection of payment info.

[9]National Highway Traffic Safety Administration, Preliminary Statement of Policy Concerning Automated Vehicles, released May 30, 2013. http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+Department+of+Transportation+Releases+Policy+on+Automated+Vehicle+Development

can choose to cede limited authority over a primary control (as in adaptive cruise control), the vehicle can automatically assume limited authority over a primary control (as in electronic stability control), or the automated system can provide added control to aid the driver in certain normal driving or crash-imminent situations (e.g., dynamic brake support in emergencies). The vehicle may have multiple capabilities combining individual driver support and crash avoidance technologies, but does not replace driver vigilance and does not assume driving responsibility from the driver. The vehicle's automated system may assist or augment the driver in operating one of the primary controls – either steering or braking/throttle controls (but not both). As a result, there is no combination of vehicle control systems working in unison that enables the driver to be disengaged from physically operating the vehicle by having his or her hands off the steering wheel AND feet off the pedals at the same time.

Examples of Level 1 automation exist today, such as parking assist applications, adaptive cruise control, or augmented braking systems.

Level 2 - Combined Function Automation: This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions. Vehicles at this level of automation can utilize shared authority when the driver cedes active primary control in certain limited driving situations. The driver is still responsible for monitoring the roadway and safe operation and is expected to be available for control at all times and on short notice. The system can relinquish control with no advance warning and the driver must be ready to control the vehicle safely.

Examples of Level 2 automation are not in existence today but can be envisioned to be applications that would combine functions such as braking and steering, for example for lane change control, or crash avoidance applications.

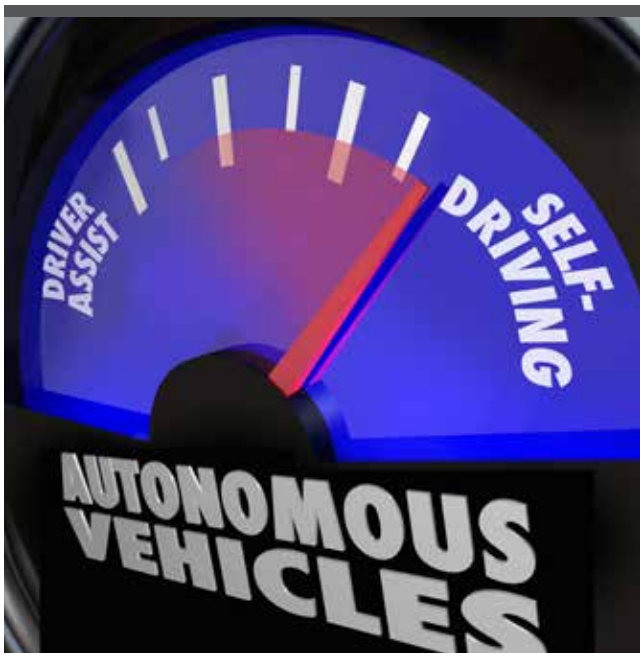
Level 3 - Limited Self-Driving Automation: Vehicles at this level of automation enable the driver to cede full control of all safety-critical functions under certain traffic

or environmental conditions and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver control. The driver is expected to be available for occasional control, but with sufficiently comfortable transition time. The vehicle is designed to ensure safe operation during the automated driving mode.

The evolution from Level 2 to Level 3 automation occurs when full control of the vehicle is ceded to the system (multiple functions and applications at once).

Level 4 - Full Self-Driving Automation (Level 4): The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates that the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip. This includes both occupied and unoccupied vehicles. By design, safe operation rests solely on the automated vehicle system.

Based on these descriptions, one can distinguish between those levels of automation that must be under direct consideration by state policy makers. Of impor-



tance and current need for attention based on the estimated timing for deployment are those technologies that imply connectivity and communication with other drivers and with roadside or centralized infrastructure and operations. Similar to the questions presented above about security for connected vehicle systems, a set of state-level principles and/or requirements should be developed that will guide both the technical and policy development areas.

Key Elements that May Influence Policy and Oversight Imposed

A few key elements that will need to be considered that influence the extent of policy and oversight that states might want to impose on automated vehicles as they emerge are included here:

- Is the automation technology entirely within an individual vehicle? (i.e., braking assist, parking assist, adaptive cruise control based on vehicle sensors).
  - This is relevant because if there is no communication between a vehicle and other actors (vehicles, roadside equipment, central transportation organizations, etc.) the extent of state regulatory oversight or policy authority related to security may be limited. State authority or policy decisions may be limited based on the state's current policy infrastructure and reach of regulatory authority as already established by state principles, frameworks, constitutions, etc. For example, one can envision a state that limits its own authority to regulate security for functions or applications that are "closed" systems within a vehicle and don't impact other actors.
  - State legislators must be cognizant of the differences between security needs and other implications of technologies. For example, states may want to limit the ability of vehicles to perform automated functions if there is a strong belief that those automated functions can have a negative effect on other drivers. Nonetheless, this would not be a security need, but rather a level of guidance or oversight on the operations of particular technologies and users.
- If the "automated" vehicle has self-driving ability, in what context is that appropriate and how does one ensure security at multiple levels – in vehicle, communications security, user level security, security of any data transmitted and stored, etc.?

The expectation, despite public excitement otherwise, is that fully autonomous vehicles (or self-driving vehicles) will not be ready to implement within the next decade.

The expectation, despite public excitement otherwise, is that fully autonomous vehicles (or self-driving vehicles) will not be ready to implement within the next decade. This is due to the immense complexity involved with sensing the external environment. However, autonomous vehicles in certain limited contexts can be envisioned to be ready for deployment much sooner. For example, self-driving vehicles on closed campuses, certain transit environments, long haul, highway-based transportation, etc.

- Can existing security systems (specifically for ensuring the security of communications and trust-worthiness of users) be adopted to apply to future automated vehicle situations?

Rand Corporation Report

A recent report by the RAND Corporation[10] examines the current state of the field of automation technologies and includes consideration of the various implications for policy makers at both national and state levels. It should be noted, however, that there are certain base assumptions in the report that imply fully autonomous vehicles without any connectivity, thus changing the security needs and landscape from the vision of automated vehicles requiring some amount of connectivity to infrastructure, other vehicles, and a back end security system.

The extent to which states and local transportation organizations and operators may be responsible for implementing, operating, and maintaining infrastructure needed for connected or automated vehicles is still a wide open question.

State Responsibilities and Opportunities – Questions 6 through 8

The extent to which states and local transportation organizations and operators may be responsible for implementing, operating, and maintaining infrastructure needed for connected or automated vehicles is still a wide open question. There is a presumption that additional roadside infrastructure will be needed to a certain extent. Currently, there are designs to transmit V2V and V2I applications and communications on the DSRC platform. This technology is short range and appropriate for broadcast. This limits its applicability to certain types of applications. The extent to which DSRC will be used for vehicle to "center" communications, specifically related to security, has still not been defined, and likely will not be until implementation plans are underway. States and local transportation agencies must understand the following:

- The USDOT to date has only released a decision to potentially regulate DSRC-enabled V2V safety communications/applications, released by NHTSA on February 3, 2014.[11]
- DSRC can be used for certain applications, such as V2V and V2I (of more interest and relevance to states). It cannot be used for longer range communications, and may need to be supplemented, depending on terrain, other networks and communications in an area, as well as the purpose of the applications.
- Additional communication networks, such as cellular, WiFi, and satellite are being considered by application developers and to some extent by the USDOT in research and testing of non-safety applications, as well as some V2I safety applications.
- Funding for DSRC roadside infrastructure can come from multiple sources, and creative revenue models have only begun to be investigated.

There is a need to perform additional analysis and modeling of potential revenue models to see where there are opportunities for investment in both infrastructure and hardware/software development and testing. The key consideration for states will be how any proposed application or communication can benefit the mission and goals of the state's transportation system.

Data Sharing: Potential Benefits

One such possible benefit may be realized in data sharing with existing operations. Although this area of research is very much in an early stage of development, there is an increasing focus on the data that will be generated by the connected vehicle system. Of interest and in need of exploration, and perhaps some level of standards development, are the key questions here.

Key Questions

- Who owns the data generated by a connected or automated vehicle? Do data stored on in-vehicle devices fall under current laws and court precedent related to law enforcement search and seizure, or will new laws/regulations need to be enacted?

[10]RAND Corporation, 2014. Autonomous Vehicle Technology A Guide for Policymakers. James M. Anderson, Nidhi Kalra, Karlyn D. Stanley, Paul Sorensen, Constantine Samaras, Oluwatobi A. Oluwatola

[11]http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles

- Who has legal access to data generated both by a connected or automated vehicle and by applications within the system?
- What are the appropriate uses for such data?
- What are the levels of privacy that are desired in a given system and/or for a given application?
- How will the data be stored? Will there be requirements or policies/practices related to how data are accessed and stored based on privacy principles or laws?
- How can "new" data generated within the connected or automated vehicle systems be leveraged or integrated into current transportation operations, such as those performed by transportation management centers (TMCs), etc.?
  - Efficiencies in performing certain operations
  - Increased costs related to adding more, analyzing, and storing more data
  - Additional information or knowledge that can be derived from the "new" data

The last question in the list above is more related to operations and uses of connected applications. However, if the questions about additional value that can be derived from new data sets are considered in conjunction with the security requirements, many of the policies and regulations should be relevant to the eventual value that might emerge. For example, if data can be used to discern valuable statistics, such as locations, distances traveled, patterns in driving, etc., states may want to consider guarding against what they would consider to be inappropriate use of that data by certain parties. One can also consider setting security parameters to facilitate or encourage certain kinds of innovations and uses. Ideally, security systems and requirements should not inhibit innovation and development of valuable applications and data usage, but should both protect and perhaps even facilitate such technological advances.

Managing Credentials

The ownership and operations of back-end security-related organizations that will generate, distribute, manage, and revoke credentials (in the case of V2V safety applications, those credentials will be digital certificates) will be performed by a number of organizations – potentially both private and public, or partnerships between the two. At a national level, the USDOT is still investigating the appropriate mix of organizations to perform these security management operations. The current vision is that there will likely be a mix of private organizations that can operate the actual functions, with some industry-wide oversight or governance body. States must understand what it will take to operate the security functions and organizations, for example who will be allowed or restricted from owning and operating various functional entities, and how the industry oversight will be managed and governed. These are all questions being debated currently and the assumption is that guidance from USDOT in the near future (within the next year or two) will help clarify what roles different stakeholders (including states and local or regional transportation authorities) are expected or able to play. More on this topic is discussed below in the Governance section of the report.

As noted in the initial section, the levels of security protection and standards are being developed for a national V2V safety system. However, states should take on a similar effort, understanding what the national system will ensure in terms of security and if the state would like to add to that level of assurance. Based on current technical designs, the V2V safety applications security system will provide the highest level of security and privacy. However, there are several opportunities and needs for the development of different security systems to support non-safety applications,[12] and this is an area where states should be engaged so they can assess how their particular needs and requirements will be met, and if there is a need to set forth additional policy or requirements to ensure security protections.

[12]Examples of non-safety applications include everything from mobility focused applications that may provide drivers with traffic or congestion information to commercial applications that could provide users with pay-for-service applications.

Finding: *State policy makers should seek out information in order to increase their awareness of the current and emerging ownership and operation plans for management of the security system for all applications for which they are seeking to set guidelines and/or policy requirements. This knowledge will help states determine where they may want to add to national, industry or federally mandated policies, practices, and/or standards.*

Research related to the levels of security for automated vehicles has not begun at a national level, though as noted above, individual organizations are likely examining this field. As levels of automation develop and get introduced, states must also consider how the security for these systems will maintain the same levels of protection and security assurance. As with other applications discussed herein, the levels of security for automated vehicles will be (at least in part) dependent on the level of automation and connectivity of those vehicles. In-vehicle and personal security may well differ from how they are ensured technically, because of the actors involved and the impact on the entire transportation or local system. In-vehicle security is specific to the components of the vehicle and the hardware and software that need to be protected. Personal security is a broader concept and includes protection against trackability, which could be gained through the communications with the vehicle and other actors or systems. The impact of vulnerabilities or failures (and thus security needed) on a closed system versus an open system is different based on who is connected to the element that fails or is compromised.

More connectivity and communication with other actors will imply the need for different (possibly higher) levels of security assurance. This does not minimize the importance of establishing and maintaining certain levels of security in automated vehicles even without connectivity, but likely those protections will be more vehicle-based rather than focused on the networks or back-end connected credential management system.

As levels of automation develop and get introduced, states must also consider how the security for these systems will maintain the same levels of protection and security assurance.

Finding: *Connected vehicles will be deployed sooner than will automated vehicles and thus the expectation is that security issues will be attended to for the connected/cyber realm sooner than they will be for the in-vehicle systems. Because automated vehicles will need connected/cyber security, as well as higher levels of in-vehicle security, the latter will increase in focus as technologies develop and should be the focus of state lawmakers' research and decision making as we move beyond connected vehicles.*

Privacy

Much of the work on design and development of security systems for connected vehicles thus far has included an explicit focus on privacy protections. As with other national systems or policies, the federal role in protecting individual privacy is limited in scope and reach.

The Privacy Act of 1974 provides a standard definition of privacy: "Any item, collection, or grouping of information about an individual … that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual." In contrast, information that relates only to vehicles, such as the VIN or license plate number, is not usually considered personal information in the United States. However, once a VIN or vehicle license plate number is associated with an individual (for example, in Motor Vehicle Department records), it may become personal information and consequently be covered under federal privacy laws. States will have the opportunity to examine and add to the national privacy protections as the connected and automated vehicle systems develop. Two fundamental questions related to privacy protections have been proposed below to guide the discussion about how states can ensure privacy is protected at the levels required.

The USDOT has determined, as part of its research and development focus areas, that "appropriate" protections on user privacy must be ensured by the security system.

Privacy Protection Questions

1. Will the national system provide privacy protection for users? At what level? How?
2. Can the states add more privacy protections or regulations to augment any national or federal requirements?

The language on the principles document states:
The connected vehicle environment will incorporate appropriate privacy controls: transparency; individual participation and redress; purpose specification; limitations on use of information; data minimization and retention; data quality and integrity; security; and accountability and auditing. For example: The environment must provide consumers with appropriate advance notice of and, for opt-in systems, opportunity to provide consent for information collection, use, access, maintenance, security and disposal. The environment will limit the collection and retention of personally identifiable information to the minimum necessary to support stakeholder and operational needs."[13]

The two main focus areas for the USDOT in terms of protecting privacy in the connected vehicle system have thus far been trip trackability and personally identifiable information (PII).

[13]http://www.its.dot.gov/connected_vehicle/principles_connectedvehicle_environment.htm, accessed: April 4, 2014.

Trip Trackability

Trip trackability refers to the ability, based on the information in the security system and from a given application, to potentially trace data back to an individual or vehicle. There is a strong focus and goal on preventing connected vehicle data from being used to reconstruct a trip made by an individual vehicle. Some work by connected vehicle researchers suggests that monitoring the Basic Safety Messages (BSM) broadcast by vehicles creates a trail of "breadcrumbs" that can be used to reconstruct a trip. The proposed privacy principles and the proposed approach for use of short-lived certificates in security management are specifically intended to eliminate this trip trackability. Other researchers have suggested that there are already simpler and less costly ways of tracking trips, such as the use of license plate recognition technologies that could be adopted if an entity was intent on vehicle surveillance. In addition, the security system for V2V safety applications has been designed in order to obfuscate as much of the data as possible, so as to guard against any one function or operator being able to piece together enough data to identify a vehicle.

Protecting Personally Identifiable Information

Automobile manufacturers may also be examining how to protect any potentially identifiable information from the vehicle within the system, based on how the devices or pieces of technology are integrated into the vehicle. Additional research is being performed now in order to identify how to integrate DSRC-based devices while isolating or eliminating the need for any vehicle-tied information, such as VIN, to be documented. Regardless of the outcomes of this research, the security credentials, as designed currently, will have no PII or other identifiable information anywhere on the digital transmissions.

State Responsibility to Establish Privacy Protection

As with other aspects of the security system, states must first understand what is included in the design for V2V safety security systems, and then examine if additional privacy protection measures should be developed. The most likely scenarios exist for additional privacy measures to be developed in policy and institutional areas, rather than in technical ones. That is to say that the current technical design of the system represents a close to anonymous system. However, policies, procedures, guidance, and other non-technical aspects of privacy protection have not been developed and likely will not be at a national/federal level. It will be up to states to develop their own guidance and/or regulations around privacy protections. This will be of paramount importance for non-safety applications that will be added to the systems. Some of these non-safety applications may even require certain levels of identifiable information, a technical requirement that states will need to pay special attention to if they are to establish privacy-protection measures that exist beyond the technical specifications.

Finding: *State legislators will need to investigate and fully comprehend the extent of the privacy protections implied by any national mandates or regulations of connected vehicle technologies. Based on an individual state's needs and mission, it should decide on any additional privacy protections it may want to regulate or mandate. Any additional privacy or security policies will need to allow for technical interoperability as well as be in line with national security policies.*

Governance

Governance, oversight, institutional arrangements, and similar topics are at a very early stage of research and development for connected and automated vehicle security systems. As part of the development of the technical design for the security system for V2V safety applications, certain organizational and institutional separations have been specified.

Because of the need for high levels of security and privacy protections, research indicates that there must be legal and administrative separation between certain security management functions. In addition, it has been recommended that industry level oversight and governance be performed by an independent, coalition-based organization. States may want to add additional protections or oversight functions to ensure compliance with their (additional) security requirements.

The questions included in the box below represent some foundational elements that must be understood and decided upon before additional state-level governance guidance or policies are developed.

Ownership and Operation of Back-end Security Management Functions

At this point it is not clear who will own and operate elements of the back end security management functions, but it is envisioned to be a mostly private set of organizations. The federal government has not expressed an interest in owning or operating security management functions or organizations, though the USDOT is interested in understanding what kind of oversight role it may play. Whether states want to take a more active or participatory role must be determined by a thorough examination of several related questions, including the following:

- What are the potential revenue or other funding models for private organizations for security management functions in which a state can participate, outside of tax revenue?
- What applications or scenarios for either connected or automated vehicle systems need state-level oversight and operation?
- What role do states want to play – oversight, compliance, operations, ownership/funding?

State-level Governance and Policy Questions

1. Who will own and operate the security back-end infrastructure?
2. What role will states play in the operation and oversight of the system within their jurisdictions?
3. Will states be able to set standards, requirements, and certification levels with their jurisdictions?
4. How can states ensure compliance with their requirements?
5. Are there any additional or new liability issues implied by the new connected and automated technologies and how might states want to respond to those issues?

- Are there ways to add value or reduce costs to other state transportation operations by leveraging or integrating with new connected or automated vehicle systems?

The legal and regulatory frameworks under which connected and automated vehicles will operate are still being developed, so the extent of state statutory or regulatory authority is still uncertain. It is fair to say that states may want to take on this set of research topics themselves, rather than wait for the federal government to ascertain where states may be able to get involved. A study that compares any state's mission and goals, vis-à-vis protecting its citizens, ensuring security and privacy for connected systems, and overseeing operation and compliance with state policies, to the technical and potential federal policy guidelines will help reveal where there exist opportunities to provide additional state-level requirements.

Status for Automated Vehicles

Of particular interest for state oversight and governance involvement are automated vehicles, as they represent a much more active set of operations and functions, than do connected vehicles, whose applications at this stage are warning or message systems, rather than actual vehicle operations systems. As vehicles progress through the stages of automation referred to previously, the need for strong policies and oversight increases. States will want to not only be active participants in testing and prototyping of the automation, but also place those new technologies and their impacts in the wider context of user security, privacy, and safety protections. Because no industry-wide institutional model exists to guide the development and management of security in the automated vehicle environment, the field is open for states (and other private or public organizations) to develop policies and regulations based on how the technologies emerge and evolve. It is unclear, at this nascent stage of research, what the implications of various automation technologies will be on states' privacy or security goals and needs.

Ensuring compliance is a matter of enforcement and oversight. Misbehavior and malfeasance detection for security systems are complex and still very much in the design stage. Fundamentally, however, what needs to be understood are the many threats and risks to the security systems for various applications, what mitigation measures exist to guard against those risks and threats, what counter-measures exist if a threat or risk is realized, and who does the oversight and checking. Auditing, regular security checks, and regular compliance of both users and security system operators may be built into federal standards or regulations, but states also have the opportunity to develop a set of guidelines or practices that can be instituted to ensure compliance with state-level requirements.

Building these checks or compliance rules into existing regulatory or oversight frameworks may well provide a chance to streamline these processes, and not place additional burden on individual users. In the absence of existing vehicle compliance or policy checks, states will have to evaluate the complete picture of risks and threats and their potential impact and probability, as compared to the burden or cost to users, the state, or other organizations to ensure compliance.

As vehicles progress through the stages of automation referred to previously, the need for strong policies and oversight increases.

One area that has not received much attention from researchers to date is that of additional liability that may be implied by new connected and automated vehicle technologies. Certainly discussions of liability implications have begun, but to date no major research efforts have been made public. We anticipate that these issues will increase in focus and importance the closer the technologies become to deployment. As with any liability discussions, the interests of multiple stakeholders, such as automobile manufacturers, infrastructure operators, legislators, and users will drive much of the research and eventual decisions about additional or new liability rules that will have to be implemented. It is unclear whether existing liability rules or precedent will apply or whether new protections or structures for deciding on liability in various situations will emerge.

Finding: *As the governance and ownership schemes for the connected and automated vehicle systems develop, state legislators will have to understand what their responsibilities or options for involvement in such schemes will be, based first on national policy, and then on intentions of the private sector. It is anticipated that there will be both regulatory options and revenue generating opportunities for states to take an active role in deciding their positions within the overarching governance and ownership structures for both connected and automated vehicle environments.*

Summary

This report summarizes the current state of the field for security systems design and policy for connected and automated vehicle environments. Both areas of study are at early stages of security system design and policy development, though there has been more attention thus far paid to connected vehicles.

Nonetheless, many of the same policy considerations for state legislators exist for both future technologies. It is an opportune time for state law makers to learn about the current research and design for providing security and to begin the process of developing policies, guidelines, or best practices that address the many challenges they face.

Concentrating on technical design, along with privacy and governance issues, will provide state regulators with a focused approach. We have begun to categorize the areas in which state-level policies or guidelines may be developed, to supplement and/or complement national polices and technical security protections. Much of the future work around security systems in these environments will depend on the scope of applications and uses that emerge for connected and automated vehicles. Maintaining a focus on a state's mission and desired security levels for its citizens can help simplify much of the complexity that is inherent with such multi-dimensional, connected, and emerging technologies and systems.

Much of the future work around security systems in these environments will depend on the scope of applications and uses that emerge for connected and automated vehicles.

Texas A&M Transportation Institute