Matthew Smith - Matthew.smith@g2-inc.com
Security Engineer
G2 Inc,
302 Sentinel Drive Suite 300
Annapolis Junction MD, 20701
www.g2-inc.com

Introduction

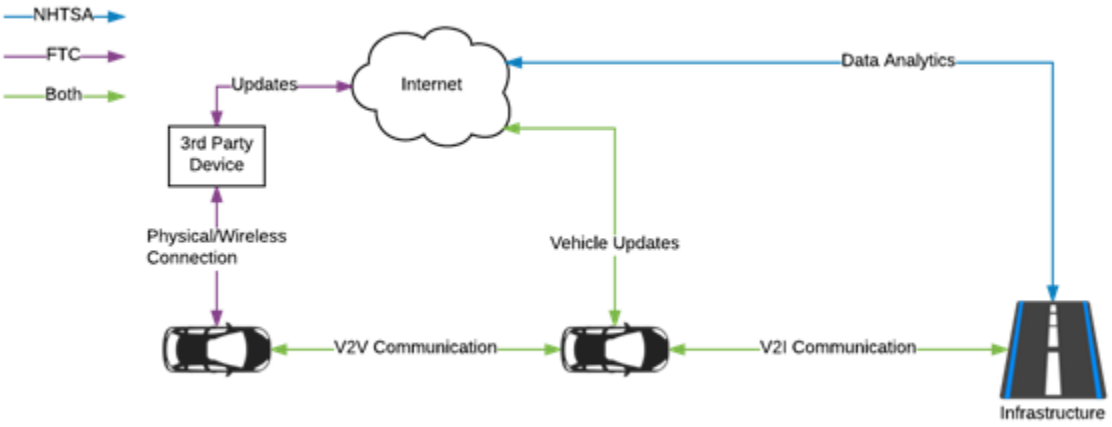
G2 is a small business, headquartered in Annapolis Junction Maryland and founded in 2001. Today, G2 employs over 130 technical personnel, has an annual revenue of ~$36M and focuses in the areas of cyber mission centric solutions and services. G2 consistently consistently reinvests corporate profits into the pursuit of new ideas, funding individual research grants, group efforts to proactively develop solutions and ultimately developing a group products that help network defenders improve the way they capture and share data. We are committed to working at the intersections of our customers. We take great pride in our role as "trusted partner" for NIST, NSA and DISA. And we look for every opportunity to help facilitate the exchange of challenges and ideas, and as solutions emerge we work hard to enable their transition to practice from the lab into mission. Over the last sixteen years, we have developed a company culture that values drive, humility, integrity, adaptability, creativity, curiosity, teamwork and recruiting and retaining employees committed to turning ideas into impact.

G2 has experience in the cyber-physical system (CPS) space. G2 has performed work under numerous federal contracts to help the government identify, assess, and manage CPS risks. As part of G2's on going support for the NIST Cybersecurity Framework, G2 has helped manage the public private partnership and industry engagement that is similar to the current process FTC and NHTSA are undertaking. G2 applauds FTC and NHTSA for working with industry stakeholders to obtain a better sense of the current landscape in automated vehicle technology.

Problem Scoping

Automated, V2V- and V2I-enabled, and other connected vehicles (i.e. with some form of wireless connectivity) can provide important benefits to consumers and have the potential to revolutionize motor vehicle safety. There are a multitude of drivers for moving to an automated fleet of vehicles. However, the security and privacy risks should be identified, assessed, and managed before a large scale roll out is undertaken.

The first step to solving any problem is to identify and scope the problem. Figure 1 below is an attempt to categorize the major types of communication that would be present in the near future of automated, V2V- and V2I-enabled, or other connected vehicles. While this figure is simple, it shows that even a rudimentary attempt to draw boundary lines between organizations is difficult in the space as there are multiple parties with jurisdiction. Therefore, before undertaking a large-scale roll out of automated technology, G2 recommends that FTC and NHTSA first define the scope and nature of the problem.



In scoping this problem, G2 recommends that FTC and NHTSA develop a similar, high level picture that identifies the types of interactions that are expected in the system and which organizations are key stakeholders in those interactions. G2 further recommends that the explicit assumptions are made clear by FTC and NHTSA i.e. the problem at hand is only related to cars, not planes, trains or aquatic vessels.

Scoping this problem also includes adding the context in which the problem resides. Some considerations should explicitly defined as part of that context. For example, the threat model for these systems should be stated clearly. If a particular threat actor has physical access to the vehicle, the data security and privacy concerns that are put in place are most likely moot. Therefore, the threat model under consideration would NOT include physical access to the vehicle. Other examples of contextual considerations include but are not limited to: technology available today, technology available in the near future, backwards compatibility with older vehicles, driver concerns, passenger concerns.

The last piece of the scoping discussion is developing objectives and a principled approach to the solutions. This stage of the process allows FTC and NHTSA to be clear on the ways in which they will make decisions on topics in the future. G2 recommends that the following objectives in order:

1. Safety
2. Security
3. Privacy

G2 recommends the following principles be adopted by FTC and NHTSA to achieve those objectives:

- Principle: Fail safe
    - The prevention of loss of life should be the number one principle for this effort. When unrecognized input is given to a particular control unit, the unit should fail safe, in order to prevent human loss.
- Principle: Least Privilege
    - As more “smart” components make their way onto the vehicle, the communications, and commands, being issued also increase. In order to make sure that commands are issued only by those with authority, each component should be designed with the minimal

amount of pre-authorization to issue commands as necessary. For example, the "infotainment" system should not be able to give a command to the brake system or the acceleration system.

- Principle: Data Minimization
    - As computers make their way onto vehicles that amount of information that is collected, stored, and generated on those systems increases. When discussing the V2I or V2V communication, the amount of data transmitted should be the least amount possible to complete the function.

Other principles may arise during the RFI and workshop and should be considered.

Answers to Questions

What data do vehicles with wireless interfaces collect/store/transmit, and how is the data used and shared?

The data needed to understand the current state of the vehicle is collected onboard the vehicle. The data is analyzed and a subset of this data is used to relay the current state to other devices (infrastructure and vehicles) in the area. Objectively, the data sent offboard would be time-based and consist of Lat/Lon, speed, direction, a unique vehicle identifier, and current safety state. The current safety state is related to tire pressure, internal vehicle temperature, number of occupants & other data which may be needed in case of an emergency situation in the near future. An example of an extension would be to include telemetry of child safety seats. Having this data in real-time would aid in the prevention of accidental deaths of infants, which is occurring more and more frequently, by transmitting this data to the infrastructure and alerting first responders of a dangerous situation where a child is present in the vehicle.

This data should be used to assist the infrastructure and other vehicles in making determinations about safety state of all vehicle traversing the area. This data is time-based and of little use beyond a certain timeframe, unless a safety situation arises. The suggestion is that there be a 5 minute rolling window of collection on the infrastructure side. There is little need for the vehicle to capture and store data, as the most important reason for receiving data from other vehicles is used in the determination of current safety.

It is suggested that the data from the vehicle be broadcasted in an omni-directional fashion to allow for the largest consumption of the data. This presents a problem in that the receiving vehicle must understand what data is necessary to update their safety state. All other data should be able to be readily discarded or dropped from further processing. This allows for quicker updates to the receiving vehicle's safety state.

How do these vehicles integrate data into their functionality? How do consumers benefit from the collection and use of their information?

Operator intervention should not be eliminated from the decision making process, this will require providing state information to the operator in an unobtrusive way. Existing warning systems, such as system indicators are well established. The addition of the state information could be relayed to the

operator in a manner that is currently in use by military flight systems, such as heads up displays and software based information panels.

Data usage is always a privacy concern, but currently insurance companies are offering a way to track the user's safe operation of the vehicle to determine insurance rates. There could be a way to passively collect information about the vehicle's state and with owner's consent have that data be used for other purposes, such as updating traffic control devices timing.

What are the current roles of vehicle manufacturers, parts suppliers, technology companies, and other stakeholders in collecting data and ensuring security? How are these roles expected to evolve?

The current role of vehicle manufacturers, parts suppliers, technology, companies, and other stakeholders is uncertain. Currently there is no good law around software or CPS liability. In this case, the FTC and NHTSA are operating in an industry with a self-regulation model. These models can be difficult to maneuver given the market forces.

G2 recommends providing clear roles and responsibilities to each stakeholder to set the basis for "reasonableness." Examples may include:

- Parts suppliers are responsible for fail safe devices
- Vehicle manufacturers are responsible for maintaining the privacy of consumers
- Integrators are responsible for know vulnerability mitigation
- Integrators are responsible for their cyber supply chain

It is expected that these roles and responsibilities will evolve over time as the components become more integrated and new functionality and technology create new operating models. The NIST Cybersecurity Framework could serve as a useful tool for developing the outcomes that each stakeholder is responsible for achieving. FTC and NHTSA could be responsible for setting the profile for each stakeholder and letting the particular stakeholder attest to how they are achieving a specified outcome.

What are the vehicle manufacturers' privacy and security policies and practices? How are those policies and practices communicated to consumers? What choices are consumers given about how their data is collected, stored, and used? Who owns the data?

What, if any, privacy and security harms can arise from connected vehicle manufacturers and their service providers' collection and use of data? What is the likelihood of such harms?

While many manufacturers and services providers collect data on users that may not harmful, the aggregation of that data may prove harmful. Location data (Lat/Lon) is not a security or safety concern until combined with personal data and time data. When those three are combined, it poses a safety concern for the user. Therefore, it is critical to keep these data points separately and limit the amount of communication between the components in which the data is stored.

Another threat vector could be identity theft. If the "info-tainment" system is asking for user input or and receiving over the air updates, the user's information is potentially at risk. A logical extension of this threat vector is credit card data. These types of interactions should be carefully considered and weighed against the risk of theft.

G2 recommends that these threat models, and others, be constructed as part of the problem identification and scoping discussion.

What privacy and security issues might arise from consumer operation of connected vehicles, including use of third-party aftermarket products that can plug into vehicle diagnostic systems, geolocation systems, or other data-generating aspects of connected vehicles?

3rd party aftermarket products produce the largest threat vector in the current formulation of the system. These products are typically not subject to regulation and may contain malicious code or be vulnerable to easy attack. As most 3rd party aftermarket products would be connected to the "info-tainment" system, the principle of least privilege should be considered most heavily in that system.

A host of issues may arise from the coopting of information gained from the system through 3rd party exploitation.

- Signal jamming could cause crashes
- Replay attacks could cause crashes
- Escalated privilege to motor/steering/speed control could cause safety/security issues
- GPS hijacking could cause navigation systems to direct vehicles to the wrong destination
- etc.

A key stakeholder in this overall system is the vehicle maintenance providers. These stakeholders possess physical access to the vehicle and directly interface with the control units. G2 recommends that FTC and NHTSA carefully consider the interaction of these stakeholders with the V2V and V2I communication components and networks.

What evidence exists regarding consumer perceptions of connected vehicles and their data collection and use practices?

What are the roles of the FTC, NHTSA, and other federal government agencies with regard to the privacy and security issues concerning connected vehicles?

As mentioned above, the first step is to clearly scope and define the problem. Then determine communication flows for the system. Then decide who has "jurisdiction" over each flow and what types of protections are needed for each flow. These protections may vary as the threat models and risk scenarios are different.

G2 recommends FTC and NHTSA consider developing clear lines of roles and responsibilities with the input of industry. The main cause of delay in security is that the processes and procedures are not well defined. G2 further recommends that FTC and NHTSA involve appropriate government agencies as early

as possible to determine their roles and responsibilities. At a minimum, this involvement can help ease the regulatory burden of conflicting or burdensome requirements. Harmonization is key to efficiency. From this harmonization, coordinated activities, like this RFI, can continue and move forward with buy-in from all stakeholders.

What self-regulatory standards apply to privacy and security issues relating to connected vehicles?

The NIST Cybersecurity Framework has played a major role in helping sectors identify opportunities for collaboration and self-regulation. There may be value to assigning specific outcomes to government agencies or industry groups through the use of Framework profiles. These high level profiles could serve as the starting point for discussions with vehicle manufacturers. For example, if PR.DS-2 (data in transit is protected) is assigned to vehicle manufacturers, then the manufacturers can take that to their respective supply chains to understand how that outcome is being achieved. Concurrently, if PR.DS-1 (data at rest is protected) is assigned to component suppliers, the conversation can be had on "what makes sense given our threat model?"

These collaborations can be industry-industry or industry-government. The real value of assigning roles and and responsibilities, in a threat context, is the clear communication of requirements. Therefore, if something goes wrong, the industry as a collective can judge whether the protection was reasonable or not because everyone was involved from the beginning.

Conclusion

G2 thanks the FTC and NHTSA for following a collaborative model of governance. G2 looks forward to continuing the collaboration at the upcoming workshop.