The Need for Data-at-Rest in

Storage Device Privacy in V2V and V2I Communications

Robert Thibadeau, Ph.D.

The Drive Trust Alliance

www.drivetrust.com

V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communications all have pairwise sources and sinks of data that have privacy concerns. Simply mitigating privacy leaks while data is in transit between sources and sinks (transmissions and collections) of data is not enough. It is imperative that the sinks and sources of data are protected against privacy leaks in order to insure that the communications themselves are protected. This point is often forgotten to the chagrin of the network solutions providers when the sources and sinks are compromised, as they so often are, nowadays.

It is not just the data that ephemerally transits through the air, it is the data that is non-ephemerally stored in the vehicles and in the infrastructure.

A source or sink point can deal with data over a spectrum of temporal constraints. The shortest is a temporary buffer or caching of data which is quickly overwritten at a source or sink. These are somewhat less problematic from a privacy perspective at the source or sink, and more critical from a network perspective. However, as autonomous vehicles employ more learning, which either expressly or behaviorally records past data more or less permanently in a source or sink, the data source or sink storage will constitute the most egregious privacy vulnerability.

It is essential that the NHTSA and FTC should directly consider these inevitable consequences of modern digital communications between sources and sinks of data at the endpoints. It is absolutely not sufficient to ask if there is a man in the middle, if the endpoints are not secured by the protocols supporting the communications.

On the questions highlighted for NHTSA and the FTC, we propose it is essential that data-at-rest, stored in the sinks and sources, is considered. Most essentially, even if you have the network security up to par, physical possession of an automobile is, by its nature, routine and mobile. Physical possession changes among owners, operators, valets, and service all the time. With physical possession the data stored that appears on the network from time to time is available in the vehicle and to the infrastructure providers.

We therefore believe there are three requirements that the government should place on all providers' electronic storage in vehicles and infrastructure. These, quite simply, replicate what has already appeared and become industry standard in the computer endpoints and computer infrastructure. For example, all iPhones, modern Android licensed products, and nearly all cloud services (such as Google). These should not be simply left alone by the Government but should provide the citizenry with uniform protections.

The three are:

1. When a vehicle or infrastructure store is repurposed, ownership or control permanently changes hands, there must be cryptographic erasure of all the material in the vehicle that is stored

excepting the factory fresh material required to operate a factory fresh vehicle or a factory fresh infrastructure storage unit. This cryptographic erase should obey international standards for symmetric cryptography, and not be susceptible to variation in all storage in the vehicle that may contain this information or in the cloud infrastructure that may contain this information. Without this assurance, the assurance value of the cryptographic erasure in any other component cannot be measured or assured.

2. When a vehicle or infrastructure store is used by one operator or one passenger for his benefit, data on other operators or passengers should not be available and must be cryptographically protected to uniform international standards. The standards for the cryptographic protection must correspond to the same quality and uniformity as for permanent repurposing.
3. The V2I infrastructure must provide assurance of the cryptographic systems in the V2I and the vehicular systems at all times so as to provide assurance that no storage in the vehicles or the infrastructure is at risk of personal or private data leakage even if physical control of a vehicle or infrastructure storage is obtained by a third party.

Below, in taking into account our requests, we remark on each of the topics mentioned to be of interest to the NHTSA and FTC.

- What data do vehicles with wireless interfaces collect/store/transmit, and how is the data used and shared?
    - We have remarked that the data used and shared needs to include the data stored as well. Protected data should include all data not associated with the factory fresh data. The technical and commercially viable mechanisms for insuring this within storage devices are well known and employed worldwide today, except in the domains commanded by NHTSA/FTC today. It would be a terrible travesty to find officials of these agencies suggesting that they had no idea of the problems, or the solutions already thoroughly vetted in computing end-points and cloud IT for other industries. We have industry standards, already. We just need attention to the facts of cybersecurity defenses and attacks, and the technologies and industry standards that already exist.
- How do these vehicles integrate data into their functionality? How do consumers benefit from the collection and use of their information?
    - If the storage devices themselves (the flash memory, for example) self-encrypts to industry standards, then the cost to the infrastructure and to enforcing uniform protect is reasonably easy and has already been globally achieved in many situations such as nearly all cloud implementations, nearly all smart phones, and nearly all network printers and copiers that can store data. Automotive storage is almost 100% flash and rotating media storage. All forms of commercially available storage have self-encrypting technology across product lines. There is no excuse for not providing the assurances requested for privacy and security today

in V2V and V2I storage.

- 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 storage device makers currently make self-encrypting storage devices used by much of the existing computing infrastructure worldwide. We can expect aspects of current technology to evolve but these evolutions are no more serious technically than those that served to determine the distance of a meter or a second in time today.
- 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?
    - We believe the three requirements outlined in the three requirements above appropriately describe who owns the data by providing limits on its use in terms already familiar to people. This does not mean that all the laws on encryption in a multitude of practical privacy laws and regulations are settled yet, but they are, we believe, rapidly becoming settled. There will, of course, always be controversy at the edges just as there it today in taking lives and limiting freedom of speech.
- 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?
    - The harms are enormous. In particular, since Vehicles are by their nature inherently mobile with inherent losses of physical control, data-at-rest protection should be uniformly standardized to strict standards reflecting existing industry standards. It is completely wrong to assume that radio, formed in a time when there was no storage possible, is the only concern of the government. We must provide suitable guarantees which can be easily inspected and confirmed in order to provide the orderly disclosure of communications to our friends and our enemies.
- 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?
    - If all third party devices conform to the encryption requirements uniformly set, then interoperability has been reasonably applied. These should be done by Federal Standards inculcated into law, such as inculcating the

AES standards from the considerable efforts from NIST.

- What evidence exists regarding consumer perceptions of connected vehicles and their data collection and use practices?
    - The evidence we have today includes the fact that industry standard public key cryptography, which is considerably more technically complicated than symmetric key cryptography, is available in virtually all vehicles on the road today, and in the cloud systems that maintain these vehicles (largely, but not exclusively, for firmware updates). Most all SSL/TLS on the web today uses these public key and symmetric key encryption standards we believe should be legislated for V2V and V2I communication today and also incorporated for data-at-rest privacy and security protection. This is not a one vendor solution. It is every storage maker and every network card maker.
- What are the roles of the FTC, NHTSA, and other federal government agencies with regard to the privacy and security issues concerning connected vehicles?
    - We believe that without FTC/NHTSA standards, privacy for data-at-rest cannot be reasonably assured for any user of any vehicle or any user of the infrastructure.
- What self-regulatory standards apply to privacy and security issues relating to connected vehicles?
    - We believe that this is not appropriate for self-regulatory standards because the simple uniform assurances given in the three items above cannot be achieved because inevitably there will be companies that provide components that that do not provide the needed data-at-rest assurances. The only other option is to create a single car company and a single infrastructure which we believe is not reasonable.