SECURITY CONSIDERATIONS for Connected Vehicles & Dedicated Short Range Communications

ALEX KREILEIN
Cofounder & Managing Partner
SecureSet
Security Considerations for Connected Vehicles and Dedicated Short Range Communications

Alex Kreilein | Cofounder & Managing Partner | SecureSet

Abstract—For decades, automotive manufacturers tempted our imagination with innovations in design, engineering, and the possibilities of things to come. Now, we are about to arrive at the era of connected vehicles and self-driving cars soon thereafter. And as ready as consumers are for these innovations, this fusion of wireless architecture and automotive production requires new considerations. Before any launch of Dedicated Short Range Communications (DSRC), a priori considerations regarding cybersecurity must be addressed to ensure the safety of the public and the efficacy of the American transportation industry. Given the demonstrable vulnerabilities in modern and connected vehicles, mitigations must be developed to address risks to life and safety. As such, a security framework or standard ought to be developed and implemented alongside a compliance regime by automotive original equipment manufacturers (OEMs) prior to the deployment of DSRC. In this way, the automotive community can continue its legacy of safety engineering, which consumers have come to expect due to decades of diligent work by vehicle manufacturers. Vehicle security architectures are necessary to protect consumers, to protect the investment in DSRC, and to protect the future of automotive innovation.

I. Overview

The purpose of this whitepaper is threefold. First, it is to identify critical gaps in the existing security architectures of vehicles. Second, it is to discuss the inherent security and privacy concerns associated with the use of Dedicated Short Range Communications (DSRC), also known as IEEE 1609. Lastly, it is to provide methods for risk mitigation to policymakers and standards developers.

By bringing these known vulnerabilities to light, the standards body and manufacturers can more thoroughly address them. Without a robust security architecture, DSRC will inevitably fall victim to intrusion by a malicious party. This could include falsifying DSRC signals to cause accidents or traffic congestion, circumventing DSRC’s weak privacy protections to allow third parties to monitor users’ movements, or using DSRC to spread malware, among many other potential threats. It is thus in the interest of consumers and industry that DSRC work in the most secure and effective manner so that it may ease industry uncertainty about the possibility of exploit by attackers, accelerate adoption, and ensure the efficacy of future smart transportation systems.

Without action, vulnerabilities in vehicle systems pose unnecessary privacy, security, and safety risks to the public at large.

Vehicles, like many other embedded systems platforms, contain common security weaknesses. There is no such thing as “unhackable code,” “totally secure systems,” or “unbreakable software.” Decades of computer science and security have proven this. And from demonstrated exploitation of gateways, to remote code execution over wireless telematic systems, it is clear that automotive systems in particular are at risk. In fact, in years past, DARPA has awarded grants to security researchers for their discovery of security weaknesses and the mitigation thereof. This has led to the publication of key research at top security conferences such as Black Hat and DEF CON. But research must now be transformed into the context of policy that will ensure consumers safety. Without trust in that safety, investments made for the allocation of DSRC spectrum and infrastructure will be wasted as the service succumbs to the lowest common security denominator, potentially compromising the safety and security of the automotive industry and the more than 210 million American motorists.

Fortunately for automotive original equipment manufacturers (OEMs), researchers and organizations have already tackled many of the challenges of developing security frameworks for connected vehicles. As will be referenced later in this analysis, organizations such as GSMA, IOActive, Bosch, Lab Mouse Security, I Am The Cavalry, and others have laid the foundation for success and have provided frameworks that can be adopted to mitigate vulnerabilities and protect consumers. Unfortunately for consumers, this work has not been integrated into DSRC standards, testing, or a current proposal by the Department of Transportation in their efforts to integrate DSRC in all light vehicles. While DSRC proponents discuss security, they have not taken any effective steps to improve security.

This analysis recommends that NHTSA require the establishment of an industry-developed automotive security standard or compliance framework. Automotive OEMs would be required to file a statement of compliance stating that they meet said requirement for each new make and model of vehicle equipped with DSRC. This will allow the FTC to use its Section 5 authority in the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce, to enforce that automotive OEMs are meeting said framework. The policy recommendation in this paper, which is based on the framework of the Payment Card Industry Data Security Standard, can be easily adopted by NHTSA and automotive OEMs. Doing so would address or mitigate the serious security and privacy vulnerabilities discussed in this paper.
II. **KEY CAVEAT**

Securing DSRC does not guarantee the overall security of a connected vehicle. But the addition of DSRC exposes a new, additional attack surface to vehicles which may already be vulnerable through different means. Moreover, the security and privacy vectors that are specific to DSRC increase the vulnerabilities of vehicles. The nature of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2X) communication requires new, additional steps to be taken in order to ensure the efficacy of connected vehicles.

There are functions that IEEE 1609 and automotive OEMs must engage regardless of their decision to integrate DSRC. At a minimum, the framework laid out in GSMA IoT Security Guidelines must be implemented prior to the deployment of DSRC-enabled vehicles.¹

III. **CRITICAL SYSTEMS IN AUTOMOTIVE SECURITY**

Before discussing the specific threats posed by widespread DSRC deployment, it is important to provide context about the vehicle systems with which DSRC may be integrated to shed additional light on the vulnerability mitigations listed in the following sections. Adherence to these mitigations creates more than just peace of mind; it is critical for protecting the life and safety of the driver, passengers, and bystanders.

A. **Delineating Systems**

At least two targets in vehicles can be used to exploit the privacy, safety and security of the driver and passenger. These are the Electronic Control Unit ECUs and the Controller Area Network CAN(s).

ECUs are embedded systems that govern one or more of the electrical system or subsystems in a vehicle. Examples include the Electronic/engine Control Module (ECM), Powertrain Control Module (PCM), Transmission Control Module (TCM), Door Control Unit (DCU), Telematic Control Unit (TCU) and Brake Control Module (BCM or EBCM). These systems generally run on microcontrollers based on x86 or ARM architectures and often use UNIX or Linux operating system variants. This makes ECUs very similar to other Internet of Things (IoT) connected devices, which is beneficial in terms of cost and functionality but concerning from a security perspective.

ECUs are interconnected over a CAN via a bus, which is designed to allow microcontrollers and devices to communicate with each other within a vehicle without a host computer. There are two types of commonly used CANs:

1. **CAN-C** is the high-speed bus that connects the engine, brakes, airbags, and other critical functions.

2. **CAN-IHS** is a low-speed bus that connects the comfort systems like radio, climate controls, and infotainment.

Each of these systems come with their own attack surfaces. The greater the interconnection between the attack surfaces and critical control units of the vehicle is, the greater the risk. DSRC does introduce new risks. With those new risks must come new mitigations.

IV. **TOP LINE ISSUES**

The DSRC protocol not built with cybersecurity in mind. Even if it were, it would not mitigate current vehicle vulnerabilities in vehicle systems. Automotive OEMs have invested vast sums of money into safety engineering for physical environments (e.g., anti-lock brakes). But ice storms and traffic accidents have no sentience, no motivation, and no tactics. Safety engineering in cybersecurity must take into account that attackers with intentionality are different from those who are not deliberate or threats without cognition at all (e.g., an oil slick).

A. **Current Standards Efforts Can Be Improved**

While DSRC is its own attack surface, it is the opinion of this security researcher that many of security vulnerabilities in connected vehicles exist outside the scope of the air-interface (i.e., DSRC). That said, it is difficult to know if this will remain the case without the needed independent and wide-scale testing and evaluation of DSRC by security researchers. At the moment, DSRC’s American IEEE 1609.2 security standard contemplates cybersecurity exclusively through the lens of cryptography. While cryptography is critical for the assurance of message authentication, data integrity, and data confidentiality, it is in itself an incomplete security solution. While other organizations such as NHTSA and Intelligent Transportation Systems at the Department of Transportation have done laudable work, a standardized approach is needed—or at the very least, a security framework. Issues of life and safety should not be left to the market. The work of IEEE 1609.2 must be complemented by a holistic vehicle security architecture in order to assure transportation safety in the age of hacking and digital exploitation.

Standards and compliance frameworks bring certainty to new markets catalyzing “permissionless innovation,” while simultaneously protecting consumers and brands. Standards such as 802.11 or any number of the thousands of IETF RFCs have enabled permissionless innovation. The lack of an automotive standards or compliance frameworks risks the investments brands will make into DSRC and connected vehicles. Standards ensure that the road does not become a tragedy of the commons filled with cheaply designed products that would otherwise undercut the significant investments automotive OEMs are making in DSRC.

B. **A Layered Strategy for Improvement**

The current standard lacks the common concept of defense-in-depth. This classic architecture requires operators

---

to create and deploy a multi-layered security architecture. These security architectures are simply missing from many current and near-future vehicle systems. IEEE 1609.2 must develop a minimal security architecture and the automotive industry must implement said architecture for each and every DSRC-enabled model of vehicle.

C. Lack of Network Segmentation

Given that interconnection between critical and noncritical systems in many current and near-future vehicle OEMs has been proven, it is incumbent on automotive OEMs to work towards a common security architecture. Vulnerabilities discovered by researchers identify the need for continued work in the cybersecurity safety engineering of vehicle systems. Part of that necessary work is the creation of methods for properly segmenting systems meant for comfort (e.g., infotainment and temperature control) and those meant for critical systems control (e.g., braking).

One known example of insufficient network segmentation resulted in the 2015 recall of certain Fiat-Chrysler Automotive (FCA) models due to a critical systems vulnerability in the Harman-Kardon UConnect infotainment system (ICSA-15-260-01). FCA issued a voluntary recall of 1.4 million impacted vehicles to patch a vulnerability in the UConnect Infotainment system [which gave] direct access to the controls of the vehicle. A malicious party connecting to the UConnect infotainment system could without any form of authentication gain access to the UConnect system. From this connection, the malicious party could take control of connected control units and send commands to the various control systems within the vehicle.3

ICSA-15-260-01 proves that the segmentation between critical control systems and comfort systems is an ineffective veneer. DSRC, as currently planned, could dramatically worsen this already precarious situation. As discussed in further detail below, the necessary integration of DSRC into vehicle control and monitoring systems will further erode, or perhaps entirely obliterate this segmentation, and make proper vehicle security measures even more challenging to implement.

D. Lack of Systems Integrity Control

The roughly 100+ embedded systems (i.e., Electronic Control Units (ECUs)) in modern vehicles are themselves a security problem. Security researchers have been able to exploit ECUs, which has enabled tampering, privacy violations, and security vulnerabilities. Lack of supply chain and code security, often poor configuration management, and other realities make ECUs particularly vulnerable. The segmentation of ECUs from each other is also not enough to ensure resistance to exploitation. Exploitation of an ECU itself may be sufficient, depending on its function in the vehicle and on an attacker’s desired outcomes.

V. Commonalities Are Concerning

Two important realities must be confronted by automotive OEMs. These concerns are valid whether or not the automotive OEM chooses to use DSRC in a commercial setting.

A. Hardware and Software Monocultures Increase Risks

In 2014, Dan Geer, Chief Information Security Officer at In-Q-Tel, noted a new issue affecting cybersecurity that has its roots in epidemiology: monoculture. When the same component is deployed on a wide scale in many different applications, failure of that component comprises a series of systems. Those common mode failures are incredibly damaging. Remediation becomes increasingly difficult as the supply chain itself can be compromised. Hardware and software monocultures cause common mode failures such that when errors occur, fixing them takes significant time and effort because the vulnerable component (e.g., OpenSSL or x86 architectures) has been so widely deployed. Greer states:

The critical infrastructure’s monoculture problem, and hence its exposure to common mode risk, is now small devices and the chips which run them. As the monocultures build, they do so in ever more pervasive, ever smaller packages, in ever less noticeable roles. The avenues to common mode failure proliferate. While it may not be in the self-interest of the Ukrainian mob to silence the Internet, nation states in conflict may make different choices. As Stuxnet showed, even exceptionally precise targeting only delays the eventual spread of collateral damage. Monoculture leads to common mode failure and thereby complicates disambiguating hostile actions from industrial accidents.4

This is a general problem in technology and a pervasive issue in embedded systems and IoT. It also affects the automotive industry. While vehicles vary in their make and model, the underlying IT infrastructure is common. While it is certainly true that different manufacturers have different software packages, that diversity is not akin to the species diversity of the Galapagos Islands and automotive OEMs are not capturing the HMS Beagle.

The risks of monocultures allow attackers to write exploits once (or a small number of times) and deliver them across a wide array of similar infrastructure. For example, exploitation of ARM microcontrollers would allow for the exploitation of a vast field of connected devices. Exploitation of OpenSSL

---


3 Ibid.

allowed for the Heartbleed exploitation of software packages running the vulnerable version and/or codebase.\(^5\)

Separately, the recent Mirai malware attack showed the consequences of commonality in language.\(^5\) This field of research is known as LangSec. In Mirai malware attacks, the lacking diversity in passwords, combined with the lacking diversity in both hardware and software, allowed for the following:

[Attackers were able to] continuously scan the Internet for vulnerable IoT devices, which are then infected and used in botnet attacks. The Mirai bot uses a short list of 62 common default usernames and passwords to scan for vulnerable devices. Because many IoT devices are unsecured or weakly secured, this short dictionary allows the bot to access hundreds of thousands of devices.\(^7\)

Without policies and standards to combat the impacts of monocultures, the automotive sector is sure to fall victim to the same vulnerabilities that the general IT market has.

A DOT mandate that all vehicles include DSRC presents a significant new risk that vehicles could be made more vulnerable by incorporating new monocultures into automotive systems. These DSRC and vehicle infrastructure monocultures would compound problems introduced by adding significant new attack surfaces, and undermining the segmentation between vehicle systems, by allowing malicious actors to potentially compromise large numbers of vehicles with a single technique.

The Heartbleed vulnerability was not a result of a flaw in the SSL/TLS protocol widely used to secure Internet traffic, but rather a programming error (e.g., technique) in a single piece of software widely used to implement that protocol. DSRC faces the same challenges, especially given that vehicle manufacturers are likely to comply with new federal regulations mandating DSRC by integrating DSRC systems manufactured by a small number of OEMs.

The notion that DSRC will be vulnerability free is fanciful at best—the history of connected systems tells us that flaws are virtually guaranteed. That is why we must take this opportunity to minimize the potential harm of these vulnerabilities and make sure they can be quickly mitigated.

\(-\)

B. Commercial Traffic on DSRC Systems Increases Risk

To say that content of unknown provenance should be able to traverse networks whose primary purpose is life and safety is to knowingly inject risk into the equation. The reason why the Department of Defense’s Secret Internet Protocol Router Network (SIPRNet) is both physically and logically segmented from the Non-Classified Internet Protocol Router Network (NIPRNet) is so that users of NIPRNet cannot affect the life and safety mission that SIPRNet supports.

Industrial Control System networks do not also carry email, web traffic, and other consumer content because of the risks. This is not to say that it cannot be done, but rather that, if this is the plan, steps must be taken to ensure DSRC’s life and safety applications are in no way impacted by DSRC’s commercial and comfort applications. This principle applies not only from a wireless bandwidth availability perspective, but also from a cybersecurity perspective.

Perhaps the highest profile failure of segmentation to date was the 2013 Target data breach in which approximately 40 million debit and credit card accounts were exposed to attackers, and potentially stolen. The Target attackers gained access to Target’s systems through network connections to allow remote monitoring and billing of Target’s in-store HVAC systems. Attackers compromised the network of the contractor responsible for monitoring these systems, and moved from there into Target’s network. There, instead of having restricted access to only relevant HVAC and associated billing systems through effective network segmentation, they were able to access Target’s customer records including credit card information.\(^8\) Thankfully, this case does not represent a failure of segmentation between commercial and safety-critical control systems. But it effectively demonstrates the fundamental importance of network segmentation.

C. Eggs, Baskets, and Band Plans

DSRC’s plan to put critical, safety-of-life Basic Safety Messages (BSMs) all on one identifiable channel, makes effectively addressing security risks even more important. Other techniques such as spread spectrum frequency hopping and even LTE’s allocation of session data rely on multiple channels or physical resource blocks. This is a natural and well-understood basic defense to signal interception that, combined with other approaches, can create robust mitigations to known and future threats.

Static use of channels creates a single point of failure for signal interception that could compromise the confidentiality, integrity, and potentially the availability of information transmitted over DSRC. Even with dynamic resource allocation, which is included in the DSRC standard, the

---


implementation is OEM dependent. This is why an industry standard or framework addressing implementation is needed.

D. Eyes Wide Open

While it is possible to manage security concerns in mixed use environments, doing so is very complicated and costly. If DSRC is to be used for commercial purposes rather than for simply life and safety, three requirements ought to be addressed by automotive OEMs:

1. A compelling case for why commercial services must use the same mission-critical infrastructure as life-and-safety communications rather than out-of-band infrastructure (e.g., LTE, Wi-Fi, etc.) must be established
2. A framework for how to secure DSRC must be proposed, developed, vetted, and adopted
3. All DSRC-enabled makes/models of vehicles must be certified against that standard or framework

That said, those requirements specific to mixed commercial and industrial use can be avoided by using an out-of-band method for the delivery of commercial information such as an LTE radio or Wi-Fi protocol designed specifically for commercial applications.

VI. SECURITY RISK MANAGEMENT

While the IEEE 1609.2 working group has taken great pains to ensure what they view as security for vehicles, their work is not yet finished. In January 2016, IEEE published Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages. This work focused nearly exclusively on cryptographic trust models to ensure integrity and confidentiality of data in V2V and V2X communications, which are not sufficient. It lacks mitigations for the well-documented tactics, techniques, and procedures used by attackers.

A. Cryptography Is An Incomplete Solution

Crypțanalysts often note that it is rare that an attacker will attempt to directly exploit cryptography when a more accessible weakness such as a vulnerability in a system configuration, physical system access, application exploitation, or network exploitation exists. Approved algorithms, by their very nature, are mathematically provably secure. While implementations themselves may vary in terms of their security, the cost of discovering, weaponizing, and exploiting a cryptographic implementation vulnerability is high. Other attack surfaces come with similar results but lower costs. To that end, the security architecture should align itself more with the attack patterns of hackers and criminal syndicates and less with the high-consequence but low-likelihood attacks by those who would seek to exploit weaknesses in generally strong trust models.

Best practices in the field of cybersecurity promote the use of defense-in-depth. The practical idea is to layer defensive structures such that even if initial access is achieved, it is difficult or impossible for the attacker to achieve action on their target. Cryptography is part of a defense-in-depth strategy, but is far from a complete strategy in itself, which is why the current IEEE 1609.2 approach must be enhanced.

B. Risk Management Strategy

Cybersecurity is predicated on a multi-faceted system built to reduce risk at each stage. To illustrate a simple defense-in-depth strategy, an attack on a facility is depicted in Figure 1. Personnel intervene to mitigate the attacker(s). The human defenders will either succeed or fail. However, given that security equipment is also in place, the likelihood of consequences from their failure is significantly lower than it would have been without the depth of defense offered by security equipment.

VII. CONTEXT AROUND DSRC AS AN ATTACK SURFACE

Connected vehicles already exist. From vehicles with 3G and 4G connectivity to others that operate as their own Wi-Fi hotspot or pair via Bluetooth with a mobile device, we already live in the world of the connected car—though their connections are far “lighter” than the “heavy” integrations soon to come. DSRC does not change that reality, but it does
change certain key areas of consideration for automotive OEMs and regulators.

A. DSRC Is Different

DSRC is substantially different from LTE or Wi-Fi air-interface integration in today’s vehicles. The purpose of DSRC is to actively enable “safety communications contributing to safer driving...” through vehicle safety applications that use vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)” architectures. Given the goal, DSRC is used for communication between trusted environments for the purposes of relaying BSMs and other telematics to the driver and the vehicle’s critical control systems. In order to achieve this goal, DSRC functionality requires greater integration with mission-critical components of a vehicle than what is currently safely supported by vehicle system architectures.

B. DSRC Can Be Highly Integrated

DSRC differs from common wireless protocols like LTE or Wi-Fi because its function is fundamentally different. DSRC has unique functions like sending BSMs, which contain time-critical information about the state of a moving vehicle (e.g., GPS position, acceleration, steering wheel angle, brake pressure, etc.). Therefore, it must be integrated very differently into the vehicle than other communications protocols.

DSRC systems interface internally to several other systems over the CAN bus to relay data and enable the vehicle to take action on DSRC messages such as BSMs. It is likely, however, that DSRC data integrates into a physically or logically common Layer 2 or Layer 3 network controller for all communications within a vehicle. While DSRC traffic is encrypted and passes through a gateway, the security of those transmissions is dependent on the security of the network controller and gateway infrastructure.

To say that because data is encrypted it is inherently secure is to ignore the realities that common vulnerabilities reveal. It is always prudent to act as if all communication is hostile and arbitrarily chosen by an attacker. For example, it may be possible to cause a DSRC device to transmit malicious BSMs (e.g., messages falsely indicating a stopped vehicle immediately ahead) merely by feeding false messages over the CAN bus (or a simulated CAN bus). Or, separately, an attacker could transmit DSRC messages designed to exploit flaws in common DSRC systems, much like the malformed ‘heartbeat’ message did in the Heartbleed exploit. As communications with unknown parties increase, so does the likelihood that attacks will exploit vulnerabilities. This is specifically why non-safety commercial use of DSRC is so concerning from a security perspective. The limited use of DSRC for only BSMs already presents a number of security concerns, primarily by, in principle, exposing vehicle systems to a new wireless interface—adding new attack surfaces while undermining proper network segmentation. But permitting commercial DSRC traffic compounds these concerns dramatically by permitting communication with a wider number of unknown third parties through a wider variety of different message payloads, all for comparatively minimal commercial benefit.

VIII. VEHICLE VULNERABILITIES

A host of powerful and important steps have been taken in the security research community by both corporate and independent security researchers to support better vehicle security. Their efforts have gathered empirical evidence used in the development of this analysis. Unfortunately, DSRC has not adopted these well-supported security practices.

A. Lacking Segmentation

In their 2015 DEF CON presentation as well as in subsequent publications, Dr. Charlie Miller and Mr. Chris Valasek demonstrated how to exploit the CAN bus through lateral movement between systems, beginning at either the air interface or a physical interface.

We speculated that if the Radio could be compromised, then we would have access to ECUs on both the CAN-IHS and CAN-C networks, meaning that messages could be sent to all ECUs that control physical attributes of the vehicle. Remote compromise of the head unit does not directly lead to access to the CAN buses and further exploitation stages were necessary. With that being said, there are no CAN bus architectural restrictions, such as the steering being on a physically separate bus. If we can send messages from the head unit, we should be able to send them to every ECU on the CAN bus.

While automotive OEMs claim that the radio and CAN-C networks are air-gapped, it turns out that is not the case in all vehicles, and it is not required by DOT or by the DSRC standard. Neither Secure On-Board Communications nor Secure External Communications are inherently present in vehicle architectures. If this were the case, the ICSA-15-260-01 vulnerability would not have existed, the FCA recall would not have happened, and the uncertainty for both Fiat and consumers would have been completely avoided. Outcomes like this cause uncertainty in the market amongst both consumers (who may be wary of owning DSRC-enabled vehicles) and amongst automotive OEMs (as to whether or not the risks are worth the reward).


12 Note: The manner and style of integration of DSRC into the vehicle is OEM dependent and may vary.

The Open Multimedia Applications Platform (OMAP), commonly found in the ARM architecture, often connects via Serial Peripheral Interface to the Motor Control Unit. This unit interfaces with the CAN bus for both CAN-C and CAN-IHS. Miller and Valasek found that the OMAP chip, on which they gained code execution via an exploit, cannot send CAN messages. “It can, however, communicate with the v850 [CAN controller] chip which can send CAN messages.” So while these systems are unrelated and not integrated onto the same chip, the exploit of one system can provide for the exploit of another through lateral movement, basic reverse engineering, and a common understanding of vehicle systems.  

B. Systems Interdependencies

In order to defend these mission-critical systems, it is important that we recognize that vehicle systems are both highly interrelated and highly interdependent. In 2010, researchers from the University of Washington and the University of California San Diego published an important work entitled Experimental Security Analysis of a Modern Automobile. Therein, they brought this acute point into specific relief:

> While it seems that such buses could be physically isolated (e.g., safety critical systems on one, entertainment on the other), in practice they are “bridged” to support subtle interaction requirements. For example, consider a car’s Central Locking Systems (CLS), which controls the power door locking mechanism. Clearly this system must monitor the physical door lock switches, wireless input from any remote key fob (for keyless entry), and remote telematics commands to open the doors. However, unintuitively, the CLS must also be interconnected with safety critical systems such as crash detection to ensure that car locks are disengaged after airbags are deployed to facilitate exit or rescue.  

This interdependency complicates the challenge of separating mission-critical and comfort systems in a vehicle, illustrating that interaction between those systems is more than a matter of expediency for automotive OEMs. DSRC, as explained above, increases these interdependencies, compared to less integrated in-vehicle systems based on LTE or Wi-Fi, creating new privacy and security challenges.

C. The Case for A Standardized Security Framework

While these vulnerabilities are indeed the case for many vehicles, this level of analysis varies by manufacturer. The vendor-dependent nature of these vulnerabilities represents a serious problem for consumers: most buyers have no way of knowing if their OEM has put in place best practices for the disaggregation of systems. This problem speaks to the need for governance and compliance such that consumers can make informed decisions about the electronic security of their vehicles in a transparent fashion.

The optimal outcome is to eliminate the need for guess work on the part of the buyer and instead develop a framework for vehicle security and a set of requirements that ensure compliance with that framework. Without those frameworks and requirements, those people with the least economic and technical agency will be inherently disadvantaged and put at risk. Put bluntly, standards protect consumers. The Payment Card Industry Data Security Standard (PCI DSS) does not only protect businesses—it protects all those who use credit cards. PCI DSS did not restrain the permissionless innovation of PayPal, Square, Apple Pay or the modern FinTech industry. Rather, it provided boundary conditions to protect innovators and consumers. If we are to ensure DSRC survives its infancy, the bar for vehicle safety must be at least as high as the bar for swiping a credit card at a baseball stadium.

IX. ATTACKS ENABLED BY POOR SECURITY IMPLEMENTATION

The use of DSRC is not predicated on the implementation of any particular security architecture. Because IEEE 1609 does not contemplate defense-in-depth techniques, all five of the categories of attacks listed below are well within the realm of possibility.

A. Deception Attacks

Attackers may spoof their location, send bogus traffic information, forge their identity, speed, and/or location, and otherwise attack the integrity of data. As documented by Tim Weil in Securing Wireless Access in Vehicular Environments (WAVE), while the motivation of attackers varies, the accuracy of information is still difficult to ascertain.

Research in this area has already been undertaken with demonstrable results. André Weimerskirch notes that “attacks on a DSRC radio can be mounted by manipulating the DSRC radio’s input and by manipulating sensor output or by injecting manipulated data packets to the vehicle’s...

---

14 Ibid.
17 Ibid.
communication bus (e.g., via the easily accessible OBD-II port)\footnote{Weimerskirch, André. "V2X Security & Privacy: The Current State and Its Future." Escrypt Inc. (2011).}.

One such attack based on sensor manipulation might be to forge the Emergency Electronic Brake Light (EEBL) outputs. EEBL messages are dependent on a number of factors (size, weight, velocity, etc.) that the vehicle broadcasts over DSRC. If those EEBL inputs are altered, all of the benefits of DSRC can be used as a weapon for attackers seeking to put lives at risk, create targeted congestion, or simply wreak havoc on the roads. By altering the EEBL inputs, the underlying data and output telemetry of a heavy truck could be altered to transmit forged information causing the multi-ton truck to appear to be a tiny Smart car. DSRC encryption techniques do not preclude this type of attack because they provide no means of validating the input to the DSRC system on which those encrypted, and therefore trusted, messages are based.

B. Denial of Service

Attackers can send false messages with a DSRC transmitter to spoof, jam, or DoS both V2V and V2X systems. If attackers can gain access to the DSRC transmitter, malformed packets can be sent between vehicles. Attackers can also increase the signal-to-interference noise ratio, and take other offensive actions to deny the availability of DSRC communications. While blacklists can be created, they assume that cars are always connected and that bad actors can be found.

As no internal vehicle security architecture exists in a standardized or compliance-oriented format, it is absolutely conceivable that vehicles will suffer from the same ills as their smaller traditional IoT brethren. The recent Mirai malware attacks against Amazon Web Services, GitHub, PayPal, Twitter, Spotify, and many others demonstrate the need for Secure On-Board Communication, and Secure External Communication all as a method to combat utilizing the processing and communications power of vehicles in malicious botnet and distributed denial of service (DDoS) attacks. Moreover, unless the infrastructure in a V2X environment is securely deployed, remotely deployed and all too often unmanaged infrastructure could be the undoing of V2V communications. Therefore, easy, safe, and secure methods for over the air (OTA) updates are required. To its credit, IEEE 1609.2 has addressed a large portion of this through their work in cryptography. However, as described above, cryptography in itself is not a complete solution.

C. Cryptographic Exploitation

While use of a Certificate Authority is specified in the standard, and all certificates are natively valid for 3 years, private keys can still be accessed through the OBD-II port in the vehicle. As OBD-II has physical access to the CAN-C and to the trust zones where keys are handled, an attacker with physical presence has the ability to overcome authentication mechanisms in ways similar to privilege escalation in a classic Linux environment. Unauthorized access to private keys allows the attacker to engage in masquerade attacks defeating not only the trust in a V2V environment but also the trust with V2X infrastructure.

Moreover, while a certificate deprecation method does exist in the IEEE 1609.2 standard, no process exists for tying the lifecycle of the vehicle to the certificate itself. For example, if a crash occurs and a vehicle is rendered inoperable, no mechanism exists to prevent an attacker from stealing the trust modules, affixing them to a new vehicle, and masquerading as the legitimate actor. While a certificate revocation list does exist in the standard, its initialization is predicated on mechanics, state Department of Motor Vehicle employees, or individuals beginning the process of revoking a certificate. To say the least, it will require a massive education and training program to ensure that these third parties, whose jobs ordinarily have nothing to do with cryptography or cybersecurity, actually take the steps necessary to revoke the appropriate certificates (and, simultaneously, not erroneously revoke others). And they must do so reliably if the certificate revocation mechanism is to be remotely effective. In the absence of such programs, as well as systems to monitor compliance, however, it is difficult to take seriously the idea that a safety critical system could depend on these certificate revocations. Any time humans are required to take affirmative action in a system, vulnerabilities (e.g. lack of training, ulterior motives, etc) are introduced.

Technology, not only people, may also be an issue at hand. The use of the Elliptic Curve Integrated Encryption Scheme (ECIES) is specified as the design choice for cryptographic assurance through IEEE 1609.2 in the selection of ECIES-256. That is the most effective choice from a cryptographic perspective. However, ECIES-256 is very computationally expensive, which poses significant problems for vehicles in transit. It is highly likely that it could take substantial amounts of time for vehicles to process and verify the cryptographic authenticity and integrity of a message. At speed, the responsiveness to BSMs is incumbent on the rate at which processors can decrypt and verify information. While low latency crypto-accelerators for ECIES-256 do exist and can be used in automotive environments, nothing requires automotive OEMs to implement such solutions. A standard or framework would address this.

Attackers could easily exploit this opportunity by sending false DSRC messages, which in turn would monopolize the processing capabilities of the vehicle and serve as a denial of service attack. Quick reaction times are especially important while traveling at a high rate of speed. This increases the need for Field-Programmable Gate Arrays and other hardware based accelerators for the computation of cryptographic algorithms. This problem could likely be solved in a slightly more sophisticated encryption approach: AES is more computationally efficient and can process cryptographic
material in a matter of mere moments. These keys can be pre-loaded into the vehicle in a trusted zone or used in consort with ECIES transmissions in an envelope approach wherein ECIES-256 initially encrypts the AES-256 crypto material, which is used thereafter to optimize around the specific challenges with vehicles.

Finally, it will not always be possible for DSRC systems to verify the certificates that the DSRC encryption scheme uses to guarantee trust. This could mean that vehicles traveling in rural areas, or which otherwise lack Internet connectivity, may not be able to connect to a DSRC Certificate Authority to confirm that the certificates used are actually genuine. To increase quick reaction times while traveling at a high rate of speed, Field-Programmable Gate Arrays (FPGAs) and other hardware based acceleration can be used for the quick computation of cryptographic algorithms.

D. Malware Exploitation

Given the persistent lack of integrated security architecture(s) in vehicles, nothing is stopping an attacker from using a DSRC transmitter as a secure, trusted, and persistent communications system for malware. If an attacker gained access to the OBD-II port, the attacker could inject executable code into the byte stream used for V2V and/or V2X systems. At this time, no standards-based mechanism exists to deal with a threat actor transmitting malware if the cryptographic signature is authentic and the transmission comes from a real vehicle and an authorized IEEE 1609 device. Blacklists do not address the malicious use of whitelisted devices.

Moreover, while blacklists can be created, that sort of thinking assumes that cars are always connected and that bad actors can be identified. Both assumptions are incorrect and dangerous to make. Furthermore, if DSRC is to be used for non-safety commercial use, information of unknown origin will be passed to the vehicle. This type of profile opens vehicles up to all sorts of attacks such as phishing attacks, which are highly common and highly damaging. The likelihood of an exploit kit being successfully installed significantly increases when any person or organization can send any message to any vehicle. Once the exploit is successfully installed, said exploit could enslave the vehicle and use it as a malware transmitter in V2V and V2X environments.

E. V2X Exploitation

V2X systems are of particular interest for exploitation as no requirements exist as of yet that would prevent connectivity to Internet or private cloud environments. Common tactics, techniques, and procedures used for exploiting even "private networks" can be used in this manner as well.

Wireless carriers have to deal with similar attacks to those likely in V2X environments. The initial deployment of femtocells brought on security concerns as some models were more easily exploitable than others based on a number of factors ranging from chipset design to software implementation. In their 2013 Black Hat presentation, Doug DePerry and Tom Ritter explored these exploitation processes.

Recognizing and reacting to this threat, 3GPP has changed the standard to address commensurate vulnerabilities in LTE femtocells based on the exploitation of CDMA and GSM femtocells. Heterogeneous eNodeB (HeNB) endpoints such as femtocells now must enable “a Trusted Environment inside the HeNB — built on a HW-based root of trust, secure boot, load only verified components — assure the eNB secure environment for crypto, key storage etc., and support a device integrity check on boot.” These best practices and others are recommended in Section XI.

The commensurate IEEE standard for V2X has not been addressed. LTE carriers are the canary in the coalmine for this attack. According to the research of DePerry and Ritter, as well as many others, the initial deployments of femtocells did not include these security mitigations. Vulnerable infrastructure was shipped and installed requiring certain infrastructure to be placed on an end of life schedule or updated with a significant forklift in firmware. To that end, we now know the dangers and costs involved in deploying infrastructure without the appropriate security architecture. To press on while understanding the consequences of absence of these measures is to ignore empirical data and sail blindly into the squalls.

F. Jamming and Spoofing

While less likely, jamming and spoofing the wireless communication of DSRC are still consequential attack methods often employed by less-sophisticated but highly motivated attackers. Attackers could jam critical communications or spoof information directing vehicles off course, denying/imparing service, blinding vehicles, and rendering onboard systems useless. Modern and future vehicles use wireless spectrum-based communication systems, Lidar, radar, ultrasonic and odometry sensors, Global Positioning Systems, Global Navigation Satellite Systems, and DSRC in both purely connected and in future autonomous vehicle capacities.

No documentation found in the proceedings of this research indicate that automotive OEMs have failsafe protocols in place to 1) detect and 2) manage vehicle safety in the event of either

jamming or spoofing. Given that velocity control is in part governed by location information, it is critical that these physical-layer vulnerabilities be understood in the context of connected vehicles. While said vulnerabilities are not unique to vehicles, the consequences of their failure are.

X. PRIVACY CONSIDERATIONS

As is the case with many consumer products, non-secure architectures bring about privacy concerns, as well. This section deals with addressing critical privacy-related concerns.

A. Tracking As An Outgrowth

In their 2015 DEF CON presentation, security researchers Miller and Valasek demonstrated how they were able to gain unprivileged access to a vehicle and push geolocation updates to a remote server, plot them on a map, and ascertain geolocation, speed, trajectory, as well as other kinematics data and transmit said information to an unaffiliated third party for unauthorized disclosure.23

It is probable that attackers and organizations will gain access to geolocation information from vehicles with insufficient security architecture. The following subsection further elucidates this point.

B. Privacy Lacking In Design

The IEEE 1609 DSRC standard does not encrypt the Medium Access Control (MAC) identifier associated with the vehicle. Instead, the standard rotates the MAC every 5 minutes.

Examples of technical controls in the current security design intended to minimize the risk of tracking via linking of security credential information in the unencrypted BSM include 5 minute certificates and shuffling of certificates prior to reuse.24

While it is helpful that the MAC is flipped on a regular basis, it is insufficient, as the kinematics of the vehicle don’t change particularly often. This leads to an easy correlation between the publicly broadcasted MAC and the vehicle itself to anyone seeking to circumvent confidentiality and privacy. Put simply, under current plans each DSRC-equipped vehicle would broadcast a BSM once every 100 milliseconds. But a vehicle’s position (to say nothing of speed and direction of travel) can only change so much in such a short period of time. When a new MAC address is broadcast, an attacker can deduce that the new MAC address belongs to the same vehicle as the MAC address that was closest to it in space, and moving along a similar vector, a mere 100 milliseconds ago. This information, in turn, could easily have been correlated with a vehicle’s license plate or other personally identifiable information through visual observation, compromising privacy and potentially putting lives in danger.

It is unclear to this researcher why the MAC is broadcast unencrypted. But its unencrypted broadcast substantially risks the privacy and personal security of the vehicle. It does, however, enable easy content delivery of a targeted nature, such as DSRC-delivered advertisements to vehicles.

XI. KEY SECURITY & PRIVACY ELEMENTS

The purpose of this section is to lay out key considerations on what automotive OEMs should use as a baseline for vehicle security. These areas serve key functions that regulators should integrate into policy as they are a base context for a reasonable standard of care that ought to be implemented to ensure the safety and privacy of the public.

Note: Many of the following recommendations were derived from the “Multi-Layered Security Approach for Connected and Automated Vehicles.” Moreover, others were sourced from the GSMA IoT Security Guidelines.25

A. Embedded Systems Integrity Assurance

The importance of the admirable work from security researchers who have successfully identified the vulnerabilities of low-level systems in vehicles cannot be overstated. Through the exploitation of weak integrity assurance, attackers are able to reverse engineer firmware, inject arbitrary code, and masquerade as legitimate parties. The protection, storage, and execution of secure cryptographic material and mechanisms is of primary importance. Additionally, the use of the following elements should be required in vehicles as part of a security architecture:

1. Secure flashing
2. Secure or trusted boot
3. Run-Time tuning detection
4. Secure debug and diagnosis
5. Hardware Roots of Trust
6. Executable space protections
7. Configuration management monitoring
8. Stack overflow protection
9. TrustZone partitioned between secure and non-secure processes and systems


10. Tamper resistant chips
11. OTA secure update systems

B. Secure On-Board Communication

Proper segmentation between vehicle systems is a critical best practice that must be followed. Computer interpretation of the wrong information risks life and safety. The strict segmentation of internal on-board networks also protects intellectual property for automotive OEMs and their stakeholders. As ECUs perform critical functions such as automated driving and sensor actuator data collection and interpretation, ECUs performing mission-critical functions must be segmented from those performing comfort-focused functions such as climate control. Adherence to the following elements should be required:

1. Critical systems must be actually air gapped
2. Protocols and administrative tools such as Telnet and Netcat should be removed or at least highly segmented
3. DSRC’s critical safety-of-life systems should be physically separated from any non-safety/comfort systems
4. ECUs within critical and comfort systems should be at least logically segmented
5. Cryptographic functions should be enabled as a part of internal on-board networking
6. Configuration management and continuous monitoring should be implemented

C. Secure External Communications

Analysis of attacker tactics, techniques, and procedures indicates that it is highly likely that attackers will use external communications systems (e.g., LTE, Wi-Fi, Bluetooth, DSRC) to exploit vulnerabilities in vehicles. But DSRC creates a far greater threat because of its greater integration with a range of vehicle systems, and role in crash avoidance. Automotive OEMs are likely to use OTA mechanisms to push updates to these systems. Accordingly, use of the following elements and procedures ought to be required:

1. Secure gateways and the use of domain separation
2. Packet inspection
3. Firewalls
4. Intrusion detection and prevention system
5. Routine penetration testing and analysis linked to compliance in order to ensure persistent security
6. Configuration management and monitoring

Technical solutions are also not the only solutions—though they ought to be required as well. However separation, inspection, policy decision making, and confirmation control must also be applied under a framework. Should a framework or standard be developed, adherence to it through assessment, attestation, and compliance are the only meaningful ways to assure its adoption and true implementation. Assessors, as will be discussed in Section XIII, ensure uniformity and efficacy so that all motorists can be assured of their safety and security.

D. Policy-Based Systems Connectivity

While connected vehicles are new, electronics in vehicles are not. Automotive OEMs can easily discern which systems ought to be able to 1) be in use and 2) communicate with critical systems both while a vehicle is in motion and at rest. When a vehicle is in motion, certain ECU-to-ECU and ECU-to-CAN communications are to be expected. Moreover, certain CAN-based behavior is to be expected. Automotive OEMs can create policy for connected vehicle systems that disallows suspicious and/or malicious actions.

The engineering behind Boolean-based systems is well understood. For example, intrusion protection systems take policy-based action to disallow port access by certain users, protocols, or other behavioral specifications. Automotive OEMs can take similar action to enforce the appropriate policy on vehicles by defining boundaries for vehicle system communication. The Bluetooth application stack, for example, does not need to speak to CAN-C and as such, policy-based governance can disallow said communication to prevent over-the-air exploitation methods.

XII. RATIONALE BEHIND A SECURITY FRAMEWORK

In order to ensure that vehicle security is in place, a standardized process must be in place prior to deployment of DSRC. Without such a framework:

1. Vehicles that actively risk users’ safety and privacy will be sold to consumers
2. Lack of economies of scale will harm the adoption of a security framework
3. Lower-income and low-information consumers will be disproportionately affected as no common framework exists for price-competitive OEMs to adopt
4. Attacks over DSRC will cause uncertainty, likely limiting the investment in and development of DSRC V2V and V2X technologies by private firms
5. It will be difficult for automotive OEMs to protect against liability without a standard of care to insure against
6. If updates are needed that cannot be implemented using OTA, infrastructure must be recalled or at least managed at dealership locations, requiring mass communications to consumers that would likely impact media coverage and the economic valuation of the automotive OEM
XIII. A Security Framework Method

This is not a new process. In 2004, the payment card industry launched a data security standard (PCI DSS), which ensures that organizations handling branded credit cards do so in a manner that increases controls around cardholder data to reduce credit card fraud. Referencing PCI DSS as a framework that the automotive community may consider, this is how NHTSA addresses the opportunity:

“Numerous real-world examples exist of organizations/systems in industries that self-govern through internal, binding contracts and agreements. Typically, such private governance is grounded in oversight and inter-organizational practices and agreements that provide the governing organization with adequate legal authority to establish and enforce industry-wide standards and maintain strong centralized functions, when appropriate.”

NHTSA is correct in that a PCI DSS-like framework could be of real value. To that end, it should be in place prior to any DOT mandate related to DSRC and certainly prior to any deployment of DSRC-enabled vehicles—to do otherwise would be reckless.

A. A Reasonable Process

In the PCI DSS context, validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm-specific Internal Security Assessor (ISA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. A statement of self-attestation is signed by both the QSA or ISA and the merchant stating that the ROC and/or SAQ meets the requirement of PCI DSS.

While PCI DSS is by no stretch a perfect system, it is one with which tens of thousands of merchants are able to comply and one which meets the key needs of consumers and the payment card industry such that security, privacy, and overall consumer expectations are generally met. A similar framework could be easily applied to the small number of automotive OEMs that design, manufacture, market, and distribute vehicles. While this researcher will admit that PCI DSS is flawed in a number of ways, the framework of PCI DSS is effective even if the standard itself is not.

In the case of automotive OEMs, compliance validation ought to be performed prior to the release of new model cars and in connection with any authorization granting use of DSRC. Automotive OEMs can use similar compliance architectures (not technical the standards) to PCI DSS and other frameworks for this. The FTC would then ensure that if automotive OEMs are using DSRC, that they are effectively implementing the security standard or framework.

B. Inputs to the Automotive Security Framework

The Bosch “Multi-Layered Security Approach for Connected and Automated Vehicles” and the GSMA IoT Security Guidelines are both excellent inputs into an automotive security framework. GSMA already gained the input of a multi-stakeholder process from automotive OEMs as well as those building the components supply chain. Bosch engaged their security approach in collaboration with multiple automotive OEMs.

Moreover, the recently published Security Credential Management System (SCMS) Proof-of-Concept (POC) Implementation Project (SCMS POC Project) sponsored by NHTSA as part of Cooperative Agreement DTNH22-14-H-00449/0003 shows real value. That said, this security researcher cannot understand practically how its implementation will occur and whether that sufficiently meets the requirement due to the length and complication of the proposal. While it may be a well-developed security architecture, it only highlights the need for all of the inputs described in this analysis, and many more, since it assumes the existence of basic security infrastructure. Surely, it is meant to work with other processes. In any event, it remains only a proof-of-concept, and will likely not be “production ready” for some time even though it appears that NHTSA is ready to “green light” the use of DSRC.

Between the proposals by Bosch, GSMA, and the SCMS POC, effective inputs into an automotive security framework are at hand. A standard or framework must be developed by the authors and contributors of stated documentation and others to allow for an expedited compliance development process.

C. Enforcement Is Crucial

The use of a compliance standard or framework tied to FTC Section 5 authorities enables enforcement action to assist automotive OEMs in their pursuit of stopping bad actors. Without a 1) compliance standard or framework or 2) a hook


into regulatory enforcement authorities, automotive OEMs would be limited in their resources for enforcement assistance.

An FTC enforcement process, in conjunction with other legal mechanisms such as the Department of Justice and NHTSA, is optimal as immediate action can be taken both from a computer security and regulatory framework. This enables both justice and market forcing functions to play at the same time, which ultimately assists automotive OEMs 1) address bad actors and 2) address bad practices components and/or implementations while serve as a referee protecting the investments of “good actors” and also protecting consumers.

This strategy addresses the tragedy of the commons that arises when vehicles of the lowest common security denominator affect everyone around them. It also reduces information asymmetries between consumers and automotive OEMs. This strategy removes the economic dependencies that limit those without economic agency from being secure. Finally, it increases the assurance and reduces the uncertainty of automotive OEMs themselves in this untested space.

D. Transparency

The current climate in the United States generally favors a light regulatory touch or even deregulatory measures. At the same time, very few people would advocate the abolition of fuel economy labels on new vehicles, food allergy warnings, drug safety labels, or other mechanisms which improve consumer choice.

That is because labeling and other transparency measures correct or prevent market failures resulting from asymmetric information between producers and consumers. Correcting this imbalance through public disclosure of cybersecurity capabilities and commitments can bolster market confidence, differentiate among market alternatives, and permit consumers to understand cost, safety, and support details – without revealing trade secrets. These improved opportunities for competition in the marketplace would also unlock systemic industry improvements, such as improved information sharing with Information Sharing and Analysis Organizations and insurers. Finally, where regulation often establishes a bare floor, transparency can promote a race to the ceiling based on free market forces.

Transparent disclosure of DSRC cybersecurity measures would therefore be a boon to consumers. But automakers have so far failed to disclose their cybersecurity practices in adequate detail. Indeed, even the most sophisticated individuals and fleet buyers such as rental car companies and large purchasing organizations such as the General Services Administration are unable to make informed decisions due to this lack of transparency.

Transparency mechanisms offer a lightweight approach to correcting such market failures, without stifling innovation, harming US competitiveness, or imposing undue costs. At the same time, they encourage adoption and improvement of cybersecurity practices by fostering the more efficient operation of free market forces.

One such existing transparency framework was published in 2014 by a grassroots security research initiative, I Am The Cavalry. Their Five-Star Automotive Cyber Safety Framework encourages vehicle manufacturers and OEMs to make attestations regarding specific cyber safety practices, intended as a starting point for free market innovation. Their framework is complementary to the NHSTA approach described in this paper, and could serve to provide different levels of assurance and detail for different audiences and needs.

E. Preemption of Anticipated Objections

It is reasonable to expect that opponents to addressing DSRC’s security vulnerabilities through a framework will make the following arguments:

Assertion: Uniform industry requirements will create uncertainty and reduce the interest in investment from the private sector.

Response: Greater uncertainty comes from the reality that the exploitation of vehicles is possible and the understanding that failing to meet a basic standard of care has consequences. A reasonable and predictable response—especially that which follows precedent set by another industry (i.e., the payment card industry)—stands to reduce overall uncertainty in the market. NHTSA’s analysis of industry self-governing frameworks is correct.

Assertion: Few attacks have been successful and thus this level of security is not needed.

Response: The number of successful attacks is, in part, a function of the vulnerabilities in the targeted system. Thus, the fact that a system has not yet been compromised can hardly be taken as a compelling argument that new vulnerabilities should not be introduced. That is precisely the situation facing would-be adopters of DSRC. Adopting DSRC without adequate safeguards could turn exploitation of vehicle systems from a rare event into one as common as PC malware—but far more dangerous to human life. Moreover, it is also impossible to know how many successful attacks have happened as event logging and reporting is not yet a practice in vehicle security. Intrusion Detection Systems are not used in vehicles to date and the Automotive ISAC is too new to have set a baseline.


 Assertion: The automotive sector is already solving these issues as evidenced by the Inputs to the Automotive Security Framework.

Response: It is true that important security documentation exists. However, white papers rarely prevent attackers from exploiting their targets. A security framework is the perfect actionable output for this good work and is needed prior to deployment of DSRC. Frameworks without compliance are little more than white papers and carry little force.

Assertion: This process will take too long and will stifle innovation, harming consumers’ ability to realize the optimized transportation experience.

Response: The recently published GSMA IoT Security Guidelines and the SCMS POC Project give a framework for how to engage in the implementation of vehicle security. Moreover, PCI DSS was quickly adopted by tens of thousands of merchants in short order. There are relatively few automotive OEMs. As such, adoption speed is dependent on the desire to address the problem quickly, not on the ability to address it quickly.

Assertion: A “holistic” IoT security regime can solve the issues of vehicle security.

Response: This objection misunderstands the vehicle-specific vulnerabilities and the unique vulnerabilities of the DSRC architecture among all other vehicle-related systems. It also ignores the immediate life-and-safety concern differentiating passenger-carrying vehicles from Internet-connected toasters. While both are important, life and safety ultimately outweighs the warming of bread.

Assertion: NHTSA alone should enforce these standards and/or frameworks.

Response: While NHTSA is the expert agency in relation to highway and transportation safety, it has less experience with protecting consumers in the domains of privacy and cybersecurity. NHTSA is the ideal agency to ensure an appropriate industry-driven standard comes to fruition. But companies who do not follow said standard or framework yet use DSRC do harm to the industry and to consumers. As such, they are deceiving consumers and engaging in unfair practices in the market. Only the FTC can ensure consumer protection in this regard.

Assertion: Because PCI DSS regulated companies are successfully breached by attackers, a standard and/or framework based on that architecture cannot be successful.

Response: While this researcher would agree that 100% of PCI DSS regulated companies that have been breached were PCI DSS compliant, that does not mean that the framework itself is to be disregarded. That argument suggests that PCI DSS is in need of an update. Moreover, the real issue at hand is that QSA industry has a hard time interpreting the standard. This is why a QSA-like function combined with NHTSA authorization sets clearer rules of the road than simply a QSA-driven process. It is hard to state that the PCI DSS framework itself is not effective.

XIV. CONCLUSION

Empirical security research already shows the general lack of security in vehicles. DSRC, as presently conceived, would make matters worse. It presents a new attack surface with special considerations, given its integration into critical control systems. The absence of security frameworks or a compliance regime risks life and safety. Providing a basic standard of care cannot be left to the market for safety-of-life systems—it is not in the case of PCI DSS, HIPPA, and a number of other standards. Without a framework, the ills of the broader IT market will be realized in vehicles, privacy and security will be risked, and the costs of security will not be easily controlled, disproportionately harming those with the least amount of economic agency.

It is necessary for the industry to ensure that the use of DSRC is predicated on the compliance with a reasonable security framework, which it currently lacks. This approach supports both motorists and automotive OEMs.

XV. About the Author

Alex Kreilein is a Co-founder and Managing Partner of SecureSet, which is a Denver, CO based cybersecurity services company. He leads the cybersecurity startup accelerator, which makes strategic investments into early state cybersecurity companies with novel products. Previously, Kreilein served as a lead technology and cybersecurity strategist at the Department of Homeland Security and as a Guest Researcher for the National Institute of Standards & Technology. Kreilein holds an M.S. from College of Engineering & Applied Science at the University of Colorado Boulder and an M.A. from the United States Naval War College.

XVI. Acknowledgments & Disclosures

This work was done in collaboration with WifiForward. Peer review of this analysis was undertaken by notable security researchers, standards engineers, and academics. Special thanks to Jake Nelson at the SecureSet Academy. My thanks to the polymorphic minds of Jacob Torrey, Don Bailey, Beau Woods, Dale Hatfield, Ann Barron-DiCamillo, Mark Althouse, and Bobbie Stempfley for their peer review of this work in addition to a host of others and for proving that cybersecurity is a team sport. Lastly, thanks to the New America Cybersecurity Initiative where I am currently also a Fellow.