The Car as an Internet-Enabled Device, or how to make Trusted Networked Cars

Gary Ellison, Jack Lacy, David P. Maher, Yutaka Nagao, Anahita D. Poonegar, Talal G. Shamoon
Intertrust Technologies Corporation
920 Stewart Drive
Sunnyvale, CA 94085 USA
{gfe, lacy, dpm, ynagao, apoonegar, talal}@intertrust.com

***Abstract*— This paper presents an overall approach to creating security and trust architecture for networked automotive vehicles and outlines basic principles for mitigating certain risks facing this new paradigm.**

Keywords-privacy; trust; security

I. INTRODUCTION

In the movie *Die Hard 4*, terrorists hack into the power grid as part of an attack on the United States. Such an attack is becoming a real possibility today, as people connect more "things" to the Internet. Unless trusted computing infrastructure is built directly into every aspect of digitally networked devices, the risk of major disruption, either via software error or malicious attack, reaches nightmarish proportions very quickly. In a world where billions of physical objects interact with network services, and with each other, the threat of major catastrophe is very real. Anyone who has experienced the nuisance of a computer virus or an outage of the Blackberry network knows how disruptive that can be, but imagine the terror of a hacker turning off the engine of every networked automotive vehicle[1] on a major highway during a nor'easter blizzard.

On a more positive note, Internet services can literally make vehicles run better. Metrics extracted from a vehicle, its driver, and its GPS system can provide vital information to manufacturers and authorities to help vehicles run better, but also plan better roads and energy management policies.

Electric Vehicles (EVs) benefit more specifically from network connectivity in a number of ways. For instance, manufacturers benefit when collecting system performance data; this is true for batteries and energy recovery systems under different driving conditions, elevations, and routes. Vehicle operators benefit from information on charging stations, and more accurate driving range information. The environment also benefits when the EV authenticates itself and its owner to the electric grid, thereby supporting new business models for time of use and clean energy based power.

Networked vehicles also represent a bonanza for marketers and e-retailers. This is not an innovation; advertisers have viewed vehicle passengers as a key target since the birth of radio, and drivers and passengers are a captive audience of music, video and games. Several manufacturers have already launched or are talking about launching "app stores" for their vehicles; others are tying the vehicle intimately to the driver's mobile phone, handing some or all of the data flow to the network operator who operate the calling plan and/or a panoply of unvetted third party applications on the driver's phone, each of which could be a virus in waiting. Ultimately, there's the driver's privacy. All of this technology opens the door to a wonderful universe of safer and happier drivers, but also turns the vehicle into one of the most intrusive collectors of private information about its drivers and passengers. A hack into data repositories on specific drivers could be phenomenally damaging to individuals. In short, the computing and network system that operates a vehicle is arguably more important than the actual engine.

The positives of networked vehicles far outweigh the negatives. The vehicle is inherently a networked machine. And the good news is that protecting a vehicle's system, the overall road safety, and driver and passenger privacy is relatively straightforward as long as the vehicle's information systems are architected from the ground up, using sound principles of trusted distributed computing. The basic principles are:

1. All components of the vehicle's computing system must be authenticated
2. Third party software and hardware must be trusted before being admitted to the execution environment
3. All personal data generated by the vehicle must be handled in a manner that is managed according to set policies and protected by access control technologies
4. All third-party services that interact with the vehicle must also be trusted and policy managed

[1] From this point on we us the term *vehicle* to refer to automotive vehicles.

5. Standard and open trust management architecture must certify that all components of the secure system and the overall architecture must have a renewable security system.

This paper presents an overall approach to creating security and trust architecture for networked vehicles and outlines basic principles for ensuring that their potential is achieved in a manner that is secure and trusted.

II. Background and Related Work

Today's vehicles support various functions that are designed primarily to provide drivers and passengers with greater safety, but also to provide convenience and entertainment. These functions include critical intra-vehicle monitors for measuring tire and oil pressure, air bag and brake status, speed/throttle status and control, and battery charge. They may also include extra-vehicle functions that gauge the proximity of other vehicles, provide collision alerts, allow for remote keyless entry and vehicle ignition, and provide basic physical vehicle access protection. Besides this, modern vehicles link to external services for vehicle status monitoring and support services, navigation support, weather and road conditions, traffic and alternative routing, location-specific information (such as nearby restaurants, fuel, battery charging stations, hotels, and shops), and other infotainment options that extend well beyond simple in-vehicle audio-visual players to real-time access to the Internet and a variety of digital content streaming services. Electric Vehicles have already integrated many of these new functions but also require battery charging support services. As the electric power grid itself becomes smarter with interconnected control systems, Electric Vehicles can take advantage of these advances as well.

In short, modern vehicles are complex, networked Information Technology (IT) systems that comprise an increasingly sophisticated array of sensors and control processors connected by internal communication networks that convey information and control signals among these sensors and processors within the vehicle as well as processors responsible for communication with services and other vehicles external to the vehicle.

The networked vehicle is becoming much more than a means of transportation. It has become an amplified personal data shadow connected to an increasingly large array of services. When we consider the vehicle as a smart phone on wheels, in the broader context of connected smart devices in the home and workplace communicating with the Internet, it becomes clear that this inter-connectedness provides more than a set of life-enhancing and protecting services. It also provides many means by which actors with malicious intentions may access a broad variety of personal information and gain control of over critical functions in the vehicle and beyond.

Over the last seven or eight years, the IT security community has begun to investigate the vulnerabilities of the networked vehicle and is beginning to work together with the automotive industry on mitigation strategies.

In a 2007 paper, Marko Wolf and his colleagues outlined in great detail the types of technologies and tools that are available for securing intra-vehicle IT systems [1] and [2]. The paper includes a very useful discussion of cryptographic primitives for confidentiality, integrity, and authentication protection. The authors advocate creating standard security modules that are implemented either in hardware, attached to or tightly coupled with Electronic Control Units (ECUs), or implemented in software, for use in less critical situations. This work has led to the creation of a group called Evita [3], which has recently published specifications for such security modules.

More recently, Stephen Checkoway and his colleagues from the University of California at San Diego and the University of Washington presented a comprehensive experimental analysis of attacks that can be levied against the networked vehicle ecosystem [4]. In their earlier work, Checkoway et al. presented a similar paper outlining attacks against intra-vehicle IT systems by attackers with direct physical access to the vehicle [5]. Their findings had many detractors, who claimed that once attackers had physical access to networked vehicles, all bets were off and that the attacks therefore provided limited additional risk. However, in their later work Checkoway et al. expanded their results to show that the same kinds of internal flaws discovered in their earlier work could lead to attacks that could be levied in a much more devastating fashion, directly from the Internet. Checkoway et al. outlined and experimentally verified attacks by adversaries with direct physical access, near-field wireless access, and long distance access.

Some of the security issues that arise when deploying networked vehicles result from time-honored manufacturing practices that have been used throughout the history of the automobile. Assumptions about the overall secure implementation of components acquired from a complex supply chain and about the software embedded in them may no longer apply in the context of vehicle as a networked IT system. The wide-scale application of ECUs in vehicles has been adopted as a means either to enhance the Safety, Security and Diagnostic (SSD) capabilities of the vehicle and/or as a means to contain costs. Suppliers design these components with exacting precision to meet the reliability and cost requirements of the OEM. To date, OEMs have not made IT security a requirement and therefore component and sub-system suppliers do not take a holistic view of the threats their componentry may be subject to in the context of a networked vehicle.

III. THE NETWORKED VEHICLE ECOSYSTEM

The networked vehicle no longer exists in a disconnected state but is part of a larger ecosystem that includes external services, other vehicles, people who may have access to those same services, and the entire vehicle manufacturing supply and support chain. It is this overall ecosystem that we must understand and analyze to be fully aware of the security and privacy issues at hand.

The typical networked vehicle ecosystem includes the following primary elements:

- Processors
  - Electronic Control Units (ECUs)[2] – These are the sensors and processors that provide status on the critical functions and respond to control signals and status information from other ECUs. Virtually all vehicle functions, with the exception of the emergency brake and steering, are controlled by ECUs. This includes infotainment systems and their connection to external services. Most modern vehicles contain tens of ECUs, and some have as many as six dozen.
- Networks commonly found in vehicles:
  - Intra-vehicle communication networks
    - Wired ECU networking (usually a variant of Controller Area Network (CAN))
    - Wireless ECU networking (such as that used by Tire Pressure Monitoring Systems (TPMS) to communicate status information to telematics systems ECUs)
    - Bluetooth for linking external devices to the intra-vehicle environment
    - Wifi
  - Inter-vehicle communication (e.g., for collision prevention support)
  - Networks for communication with external services and networks (Internet hosted services, GPS navigation, telephony, digital content services, vehicle support services (e.g., OnStar))
    - Proprietary networks
    - IP-based networks over 3G, 4G, GSM
    - Mobile telephony
    - GPS
- Software
  - There are millions of lines of code running inside ECUs and associated support systems.
  - ECUs are provided by different technology providers and typically, the software in each ECU is unknown to other ECU providers or to the vehicle manufacturer.
  - Applications downloaded into infotainment systems – In addition to ECU software, modern infotainment systems support the driver's ability to download many of the same kinds of applications that consumers download to tablets and smart phones.
- Services
  - GPS-based navigation, traffic, road condition, weather and travel information services
  - Internet hosted services (entertainment and/or applications)
  - Vehicle support services (e.g., OnStar)
- Human agents
  - Manufacturing supply chain personnel
  - Maintenance personnel
  - Vehicle owners/driver
  - Passengers

As with any ecosystem, networked vehicle ecosystem design and deployment involves intricate choreography of all IT elements in the context of the design and manufacture of the overall physical system – the vehicle itself. This includes assuring compliance with a complex set of internal product requirements and budget constraints, industry regulations, safety and security criteria, and software design requirements and testing criteria. Any analysis of the networked vehicle ecosystem must take these constraints and criteria into account together with the complexity of the ecosystem supply chain.

IV. CONNECTED VEHICLE ECOSYSTEM RISKS

Systems such as those described above that collect information about consumers, their energy usage, and driving habits raise privacy, trust, and safety issues. Similar issues have been encountered when dealing with healthcare records, smart meter applications, and a variety of applications for smart phones and tablets. A great deal of information is being collected about consumers over which they have no control. To make matters worse, it is often unclear how that information is being used and by whom.

In addition, networked vehicle ecosystems can be designed so that control signals can be sent from external services directly to ECUs. These services, the communication link between them and the ECUs, and any control data can be subject to exposure or tampering (malicious or coincidental) that can result in unauthorized control messages being sent to the vehicle. The risks here are not equivalent to typical privacy-violation risks. The bigger risks are attacks on the vehicle itself; these include denial of service attacks, manipulation of the climate controls for mischief or to drain the battery, and any number of other problems that can be caused by malware introduced into the vehicle. Other risks

[2] In the literature the term ECU is prevalent. However one also sees TCU (Telematics Control Unit) to refer to the Telematics ECU. There are also other processors that are not called ECUs. For this paper however, we use the term ECU to refer to any processor used within the vehicle.

can arise from direct tampering with the intra-vehicle information systems, which may put the vehicle into a dangerous state.

Over the last several years, the IT security community has generated numerous reports and technical papers that describe a set of potentially devastating attacks against vehicle IT systems. Such attacks can give attackers complete control of any vehicle function that is controlled by an ECU. These attacks are no longer limited to intra or near vehicle access. They can be mounted from the Internet and can be used to attack a specific vehicle or a large collection of vehicles [4]. The reports highlight that the vulnerabilities that result in such attacks are largely based on the fact that vehicles have not been designed as externally networked IT systems. This is reminiscent of the early days of the Internet, when the assumption by those connected to the Internet was that there was no reason to focus on external threats or actors with malicious intent. Before computerized controllers were used within vehicles, there was no threat of an IT attack. Today, vehicles are networked entities that exist in cyberspace much like any other computational node, PC, tablet, or smartphone. It is in the context of this overall ecosystem that we must evaluate the security risks of the vehicle IT system against attacks perpetrated from within the vehicle, close to the vehicle, or over the Internet at large. This evaluation must result in the design and deployment of measures that mitigate these risks.

Analysis of the types of attacks that can be mounted against the networked vehicle IT system focus on a variety of variables, including the following:

- Required proximity of adversary
  - Direct physical access – use of OBD-II port, physical access to ECUs and intra-vehicle communications busses
  - Near-field wireless access – access to vehicle's Bluetooth, Tire Pressure Monitoring System (TPMS), Remote Keyless Entry and Start systems
  - Long distance wireless access – access to vehicles' external communications control ECUs for subscription-based safety and security services (e.g., OnStar, Lexus Link, BMW Assist), mobile telephony, infotainment systems, and Internet access. Some of these attacks can lead to access and control of virtually any other ECU-controlled system in the vehicle.
- Goal of adversary
  - Access to and theft of driver's personal information – location tracking, financial information, conversation monitoring, general habits
  - Control and/or theft of the vehicle – Access to intra-vehicle control functions can provide means to interfere with system monitors, override security functions, tamper with safety functions including air bag systems, throttle governors, braking, or battery charging
  - Access to long distance vehicle communication channels – subscription-based safety and security services communication data, GPS tracking information, mobile telephone systems

Of these, the attacks that can be mounted from the Internet and that give access to control of critical vehicle functions are perhaps the most worrisome. However, we cannot overlook the damage that can be done by those with direct physical access to ECUs and intra-vehicle busses. This kind of access can in fact set up broader Internet-based attack scenarios when adversaries gain access to ECUs and are able to modify the ECU code [4]. The main lesson to be learned from this high level analysis and experiences associated with securing the Internet and the devices and services that depend on it, is that the vehicle cannot be treated as an independent entity. It is part of a larger community, and securing that community requires an overall awareness of how each component of the ecosystem impacts the security of other components. Fundamentally, it requires that all components exist in a trusted environment.

V. Security, Trust and Privacy Management for Connected Vehicle Ecosystems

In order for networked vehicle ecosystems to be secure and safe for drivers, all communicating and processing elements must establish a trust relationship with the elements they support or rely upon. This includes vehicle manufacturers, vehicle owners, vehicle technology component providers, network service providers, and other value chain participants in the ecosystem. Establishing trust between them requires clearly identifying and describing the following:

- All ecosystem stakeholders. These include vehicle manufacturers, vehicle owners/drivers, vehicle technology component providers, vehicle maintenance and repair personnel, vehicle support service providers, infotainment service providers, and (downloadable) application providers.
- Internal and external supply chains. Security and trust management necessarily involves an intimate understanding of the relationships among technology components provided from different sources, as well as an understanding of how adversaries and intruders can affect or attack those components and how such attacks can create downstream effects on other components.
- Technology components. These include ECUs, the interfaces between them, and software and systems based on them.
- Networks used for communication among these components.
- Inter-dependencies among the components.
- External services that interface with internal components,

- Which stakeholders must have access to which components?
- Privacy, confidentiality and usage rules associated with data exchanged between the vehicle and various networked services.

Once this ecosystem description is established, the next step is to determine the trust relationships that should exist among the vehicle IT components. For example, is the telematics ECU allowed to communicate with the TPMS ECU? Can this interaction be bilateral? Can the interaction involve control signals or is the exchange only about providing status to the telematics ECU to notify the driver? After trust relationships are established, a strategy for enforcing those relationships must be determined.

Ultimately, these points translate into the need for a framework for establishing trust among the networked vehicle ecosystem elements and stakeholders. This is called a trust management and security framework.

A. Trust Management

Trust Management systems provide answers to questions about ecosystem principals and resources and methods for establishing trust and securing their interaction [6]. These questions include:

- What principals are involved in the ecosystem? That is, what entities – people, processors, services, programs, etc. – are involved in the ecosystem as actors requiring access to other entities?
- How are these principals identified, and what mechanisms should be used so that principal identity can be trusted?
- What ecosystem resources need to be governed and protected and what mechanisms should be used to do so?
- What principals are authorized to access which resources and for what purposes?
- What entities are trusted to set policy around resource usage, ecosystem principals (including identification), and overall ecosystem deployment and management? That is, what entity or entities act as roots of trust or as Trust Authorities?
- How are related security and privacy policies articulated, communicated to relevant stakeholders and enforced?

These questions are focused on all internal and external vehicle interactions. In particular, they focus on data that are collected by intra-vehicle sensors, the entities that require access to these data, and the channels used to communicate the data among authorized entities. These data are communicated to intra-vehicle control units or to Internet-based services that are responsible for translating data into control or information signals that support the vehicle operator, network services, or control the vehicle. The principals involved in this type of ecosystem include technical components – sensors, control units, network interfaces, service support infrastructure – as well as humans with access to the vehicle and services with which it is associated – vehicle operator, manufacturing and maintenance personnel, extra-vehicle infotainment and support services personnel. At any point, if access to a resource is granted to a principal that should not be trusted with such access, potential security and privacy vulnerabilities arise.

B. Privacy Management

Personally Identifiable Information (PII) and any of the data collected by the vehicle sensors and transmitted to services must be used consistently with well articulated and user agreed privacy policy. It may be the case that some data elements will not in and of themselves compromise user privacy. However, when these data are put together with data collected via other Internet-based sources, PII may in fact be derived. Therefore, when considering privacy policy associated with collected data of the types identified for networked vehicle ecosystems, the types of issues that must be considered include the following:

- It must be clear who it is that generates data that must be privacy protected. In many cases it will be the vehicle operator/owner, but it may include passengers and in the case of rental vehicles, the owner is temporary. There have been cases in which some smart phones, when paired with the cellular interface of a previously owned or rented vehicle, gave access to the previous owner or renter's personal data.
- Privacy policy must identify and articulate those principals that may access PII and how and whether PII may be used.
- Privacy policy must specify how all data will be used and by what principals so that the PII is not compromised. This includes articulating policy associated with whether or not the initial data recipients may share collected data with other entities and if so, under what terms.
- Users must be involved in such policy making to the degree possible and the interface supporting this involvement must be simple.
- Policy must be enforced. Policy that is negotiated among owners and recipients of such data can be enforced using various techniques such as access control systems or data anonymization mechanisms that use private agents acting on behalf of the data creator.

C. Security

Implementing and deploying the kinds of information systems discussed in this paper in a manner that is secure and enforces articulated trust and privacy policy, necessitates acquiring deep knowledge of the elements involved. This includes understanding for each system element – processor, sensor, controller, or service – the processing power, the ability to store and protect secrets, whether or not the element is uniquely identifiable, support for software and/or firmware

upgradeability and renewal in the face of component breach, and a host of other functions critical to secure systems design. Additionally, the communication channels among the various system elements must be analyzed to determine channel bandwidth, access to channel inputs and outputs, and means for protecting the integrity and confidentiality of the information traversing the channels.

As described in the Background and Related Work section, Wolf, et al. covered in great detail the cryptographic and security technologies required for securing the networked vehicle [1]. We must consider the application of such technology from a systemic perspective. Two elements may interact in a secure fashion yet still compromise one another if such interaction is not carefully understood in the global networked vehicle ecosystem context. That is, beyond authentication and confidentiality we must consider authorization. If two ECUs have no need to interact, we must ensure that they cannot interact by using a background channel such as a debugging interface. If a service acquires vehicle operator location data, we must enforce that use of that data beyond the intended collecting service is extended only to those who are authorized and only according to specific policy.

In the next section we discuss these issues in greater detail linking them to the mechanism required for trust and privacy management and for maintaining the security of vehicle and service control.

VI. A Trust and Privacy Management Framework

In the last 20+ years computers, phones, tablets, and a host of other devices have been interconnected via the Internet. This has provided an array of interesting services and features that have vastly extended the power of the devices had they remained unconnected. In the early days of the Internet security was not a primary concern. But as the Web emerged along with commercial services, electronic banking, stock trading and other critical services the targets became more interesting to adversaries and Internet architects started preparing for next generations of underlying protocols and applications, giving rise to advances such as IPv6. Over the same period, researchers discovered ways to create computer viruses and other measures for infiltrating online systems and services (see for example [7]). These research viruses went 'viral' and became a major tool used and 'improved' by individuals and organizations with nefarious intentions towards Internet services and their users. This development in turn provided the impetus for companies that focus on IT security and a wide variety of tools and methodologies for securing and monitoring IT ecosystems against an ever-increasingly sophisticated array of attacks and threats.

The networked vehicle community is essentially in a place similar to IT systems 20 years ago as they first connected to the Web. There is however a major difference. There now exists the very rich set of security tools, methodologies, standards, and organizations established over the last 20 years. It is this set of tools that we need to apply to the networked vehicle ecosystem.

Such application can be discussed at a general level but as with any security architecture, the devil is very much in the specific details associated with the real system at hand. We now explore a general application of secure system methodology starting with a basic tenet that has evolved over the last 20 years – the security of the elements of an ecosystem cannot be considered independently of the other elements of the ecosystem and the ecosystem as a whole. That is, we start from the first principle that securing the ecosystem requires intimate understanding of all of its components and their relationships to one another.

A. Setup – Establish an Ecosystem Security Process

The first step in the creation of a trust and security framework for an IT ecosystem is to establish an IT security organization and chief security architect position within the manufacturing process. This individual and organization would be responsible for overseeing the application of security methodologies to the system as a whole and would interface with other supply chain managers to identify and make sense of security-based requirements in the overall production and deployment context and budget. The security architect and organization would do risk/benefit analyses for each security requirement.

The next step of the process is to create a complete IT map. This includes:

- Identifying and analyzing each sensor and ECU.
  - For each of these it is critical to know the ECU manufacturer, function, interface specifications, software and related renewal and debugging processes, and the dependencies on and communication with other ECUs.
  - What data are exchanged?
  - Who has access to the ECU and via what channels?
  - What external services interface with a given ECU and via what networks?
- Identification and analysis of all intra and inter communication networks
  - ECU-to-ECU networks
  - Wired and wireless networks
  - ECU-to-external services networks
- External Services and Service Providers
  - What services interface with the vehicle
  - What ECU is responsible for this interface?
  - What data are passed to the service from the vehicle?
  - What data are passed to the vehicle from the service?

B. *Principal/Resource Interaction Analysis*

As described in section V.A, trust management systems pose and answer questions about principals and the resources with which they are authorized to interact. The IT map must be viewed from this perspective.

- Identify principals that will act upon and require access to resources identified in the last section.
  - How are principals identified in communication with resources? How are resources identified?
  - What entity or entities vouch for these identities?
  - Determine which principals require interaction with which resources. In some cases such interactions will be ECUs acting as principals requiring access to other ECUs. In other cases, humans or services will act as principals requiring access to ECUs or services will require access to data from specific ECUs.
- Classify all resource functionality from safety critical to entertainment
  - Critical vehicle control and safety
  - Communications of system status to driver or vehicle support services
  - Telematics functionality
  - Infotainment functionality
- Create an authorization/authentication/confidentiality map
  - Which principals are authorized to access which resources and for what explicit purposes?
    - Read only access?
    - Write access (may send control signals to ECU, for example)?
    - Software update access?
  - What entity or entities authorize such access?
  - How should communication between authorized principal and resource be protected?
    - Confidentiality protected (encrypted)?
    - Integrity protected?
    - Support for message freshness?
    - Authenticated?
- Certification
  - Determine to what extent component certification processes can be created or modified to include secure software practices.
    - For example, such processes might certify that ECU interface software has been designed taking into account the other entities that might be accessing the ECU, avoiding critical buffer checking/overflow errors and other types of common programming errors that lead to security vulnerabilities.
    - This may also take advantage of existing automotive component certification processes that have been expanded to include security criteria.
  - Create robustness criteria for each type of resource
    - Certify that the resources comply with such criteria.

C. *Ecosystem Security Analysis and Framework Design*

Once it is clear which principals need to access resources and what the nature of this access is, the security team must identify technologies that are appropriate for enforcing this trusted access model. As Wolf et al. point out, most ECUs will not have the computing power to support handling complex public key signatures or decryption [1]. The security team must take this kind of information into consideration in their design.

- Analyze tools to implement authorization, authentication, and confidentiality for each resource and communication network protocol
  - Determine ECU cryptographic capability
  - Determine need for a central hardware security module, or similar functionality implemented in software.
- Design overall security and policy managed privacy architecture
  - Assign security technologies to each resource appropriate to its authorization, authentication, and confidentiality requirements and computational capabilities.
  - Assign credentials to each principal and resource
    - For example, these may be public/private key pairs and associated certificates.
  - Design interface access control for each resource
    - Principal X is allowed Y access to resource Z
    - For example, Y may be read and/or write access.
  - Design policy managed data access for all principals
    - Such a system must provide a simple interface for drivers to specify policy associated with non-safety-critical vehicle data.
    - Policy must cover issues associated with service providers that have access to vehicle data (for example, location tracking information) and the terms under which this data can be shared with other entities. For example, the driver may be provided with an interface for specifying the terms under which her location information may be shared with other services.
    - The mechanism must provide means for anonymizing collected data for services that don't actually require personal identification detail.
- Trust Authorities
  - Create a trust/certification hierarchy appropriate to the ecosystem.

- Such an authority would be responsible for creating trusted credentials for ecosystem resources and principals.
- This includes understanding what entity in the overall networked vehicle ecosystem should take on such responsibility.

D. *Ecosystem Security Testing, Monitoring, and Renewability*

There is no such thing as perfect security. Systems will be successfully attacked. A well-designed security framework must include means for breach detection and a strategy for renewing firmware and software functions when such breaches occur. The security team should plan and implement

- A threat assessment capability
- A penetration testing capability
- A vulnerability monitoring capability
- A breach management capability

VII. Security Issues Specific to the Connected Vehicle Ecosystem

As stated earlier, every ecosystem has peculiarities that make securing it different from other ecosystems. We have alluded to some of the problems with the networked vehicle relating to general manufacturing and component acquisition practices that have been used in traditional automotive systems. These practices have typically arisen in the context of physical components, the specifications for which have traditionally been provided in great detail by the component OEMs to the vehicle assembly teams. However, for a variety of reasons, ECU OEMs typically do not share software source code. One of the strongest conclusions of the Checkoway et al. paper [4] is that "virtually all vulnerabilities emerged at the interface boundaries between code written by distinct organizations." This can lead to a variety of problems since programming practices cannot be checked for well-known security holes. The security team will need to create a strategy for ECU interface software review as well as software update and renewability.

Other problems arise from the fact that the automobile has not traditionally been connected to the Internet but rather to proprietary networks, access to which has typically been limited. The automotive industry must take advantage of the last 20+ years of IT security research and experience. The experience can point not only to the practices and solutions that are most appropriate but can also help avoid the pitfalls of what may seem like simple solutions. For example, it is often tempting to place firewalls between safety-critical functionality and other non-safety-critical functions. This inevitably creates major interface and usability headaches and is ultimately not as secure as a more holistic approach to trust and security such as is proposed in section VI.

Additionally, automotive component OEMs are typically required to comply with various standards and undergo certification by associated labs. This practice must ultimately be expanded to include security. To the extent that standards can be employed, particularly with respect to cryptographic primitives and protocols and secure software practices, such compliance checking and certification can help ensure that the networked vehicle ecosystem security is well-understood, robust, and responsive to breaches.

There are certainly other automotive industry specific issues that will impact the analysis, design and deployment of trusted solutions. Identifying and grappling with these will require the two communities – the automotive industry and the IT security community – to educate one another. The sooner that this can take place the better. The alternative is the kind of patchwork response-to-attack based security that has been all too common over the last 20 years. If we've learned anything, it's that after-the-fact application of security is much harder and more expensive than integrating it from the beginning.

VIII. Conclusions

It is no secret that security and privacy are critical concerns for all stakeholders involved with the design, implementation and deployment of networked vehicles and infrastructure to support and take advantage of them. This paper highlights the vulnerabilities and risks inherent in these ecosystems and provides a trust management approach to understanding and securing the interactions among ecosystem elements and stakeholders.

IX. References

[1] M. Wolf, A. Weimerskirch, and T. Wollinger. State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems, 2007.

[2] M. Wolf, A. Weimerskirch, and C. Paar. Security in automotive bus systems. In C. Paar, editor, ESCAR 2004, Nov. 2004.

[3] http://evita-project.org/index.html

[4] S. Checkoway, D. McCoy, D. Anderson, B. Kantor, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In D. Wagner, ed., Proceedings of USENIX Security 2011. USENIX, Aug. 2011. Finalist for the 2011 NYU-Poly AT&T Best Applied Security Paper Award.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In D. Evans and G. Vigna, editors, IEEE Symposium on Security and Privacy. IEEE Computer Society, May 2010.

[6] M. Blaze, J. Feigenbaum, J. Lacy. Decentralized Trust Management. Proceedings of the 17th IEEE Symp. on Security and Privacy. pp 164-173. IEEE Computer Society, 1996.

[7] http://en.wikipedia.org/wiki/Morris_worm

[8] M. Raya and J.-P. Hubaux. Securing vehicular ad hoc networks. Journal of Computer Security, 15(1):39–68, 2007.

[9] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. Security and privacy vulnerabilities of in-car

wireless networks: A tire pressure monitoring system case study. In I. Goldberg, editor, USENIX Security 2010, pages 323–338. USENIX Association, Aug. 2010.