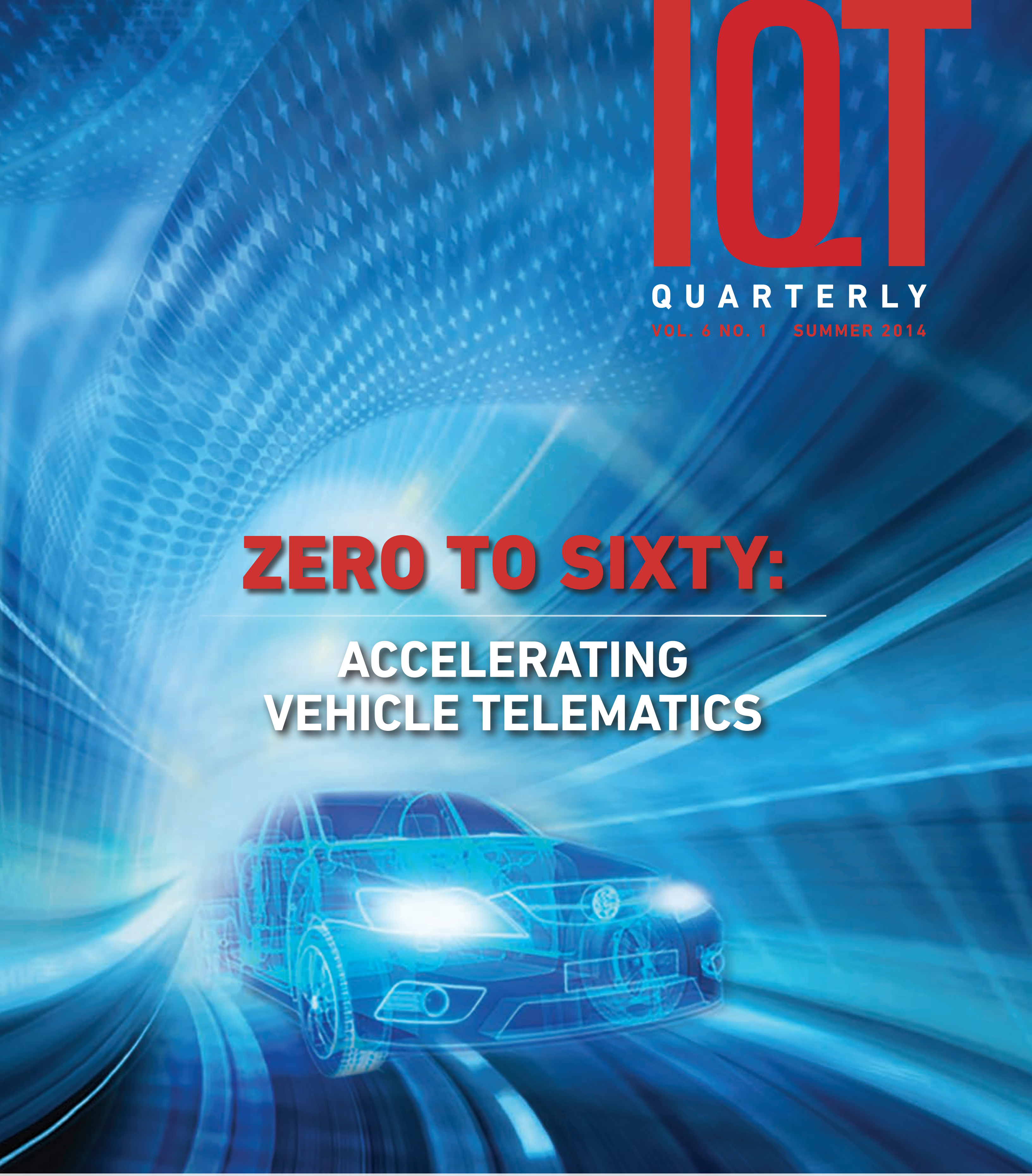
IQT
QUARTERLY
VOL. 6 NO. 1 SUMMER 2014



ZERO TO SIXTY:

ACCELERATING VEHICLE TELEMATICS

IQT
IN·Q·TEL

IQT Quarterly is a publication of In-Q-Tel, Inc., the strategic investment firm that serves as a bridge between the U.S. Intelligence Community and venture-backed startup firms on the leading edge of technological innovation. *IQT Quarterly* advances the situational awareness component of the IQT mission, serving as a platform to debut, discuss, and debate issues of innovation in the areas of overlap between commercial potential and U.S. Intelligence Community needs. For comments or questions regarding IQT or this document, please visit www.iqt.org, write to iqtquarterly@iqt.org, or call 703-248-3000. The views expressed are those of the authors in their personal capacities and do not necessarily reflect the opinion of IQT, their employers, or the Government.

EDITORIAL
IQT Quarterly, published by In-Q-Tel, Inc.
Editor-in-Chief: Adam Dove
Theme Editor: Gerry Hamel
Contributing Editors: Brittany Carambio and Emma Shepard
Managing Editor: Lisa L. Bader

Design by Lomangino Studio LLC
Printed in the United States of America

IQT
QUARTERLY

Identify. Adapt. Deliver.™

TABLE OF CONTENTS

ON OUR RADAR

VEHICLE TELEMATICS

By Gerry Hamel

For those following the Consumer Electronics Show (CES) in January 2014, it may have seemed like the Detroit Auto Show started a few weeks early. The notion of the connected car and partnerships between automakers, telecommunications providers, and other major tech companies were common themes throughout the week. Given the automotive industry's relatively slow and methodical approach to release cycles, it certainly appeared that a dramatic shift was in progress.

Interestingly, just as CES 2014 was kicking off, IQT was wrapping up a market survey of the broad automotive telematics space. In our research, we found an ecosystem tying large suppliers in the auto industry to well-known names in mobile. Under this large umbrella were companies targeting use cases ranging from fleet management and logistics to usage-based insurance (UBI) to data connectivity and infotainment. Although there have been a number of recent innovations by startup companies taking advantage of declining costs, the concept of automotive telematics has been around long enough for a clear pattern to emerge: rather than seeking to develop proprietary solutions specifically for the auto industry, chipsets and software standards from the mobile industry are being adapted to fit the needs at hand. For example, devices might transmit intermittent telemetry data through a mobile data connection and software updates might be pushed down to a vehicle using a modified form of the Open Mobile Alliance Device Management (OMA-DM) standard that was originally created for configuring handsets.

As evidenced by the announcements made at CES, the important changes occurring in this space are providing many opportunities for innovation. In some cases (e.g., self-driving cars) these developments require vast resources beyond the reach of a typical startup. Despite the barriers to entry for small companies, we do see some potential opportunities for investment in the area of vehicle telematics. More importantly, we see new technologies arriving that are likely to provide better platforms to spur this innovation. In cases like the inclusion of in-vehicle LTE hotspots, the advancements are somewhat iterative and the opportunity for disruption is not entirely clear. In others, such as the creation of the Open Automotive Alliance (OAA), major changes appear imminent.

In January 2014, Google announced the formation of the Open Automotive Alliance, perhaps one of the most exciting recent developments in this space. This organization consists of a variety of companies seeking to use Android as the operating system for in-vehicle infotainment (IVI) systems, and could be viewed as the automotive equivalent to the Open Handset Alliance. With this frame of reference, it is interesting to consider the current state of this "center stack" (tightly controlled, distinctly styled and branded) and then look back at the mobile handsets from 2006. Prior to the arrival of the modern mobile OS, carriers exercised a similar level of control over the handsets that were allowed to connect to their networks. Although it is still too early to say what the final outcome will be, it seems clear that a

When we think about vehicles with massive data pipes, extensive processing power, and a more friendly application development environment, it really seems like a new wave of innovation is upon us.

friendlier platform for automotive app development is not too far away.

Numerous automakers have begun to demo self-driving cars. While Google is probably the most well-known organization to be working on this technology, there have also been recent demonstrations or announcements from Audi, BMW, Nissan, Toyota, and Volvo. Over the past few years, more and more safety systems such as adaptive cruise control and lane-departure warning have been added to vehicles. The ability for a car to sense and react to its surroundings has steadily improved to the point where autonomous driving in the real world is just around the corner.

One new advancement that is likely to make vehicles both safer and more fuel efficient is known as V2X, a term intended to encompass both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Although there are multiple standards, these solutions rely on wireless radio communications to automatically inform vehicles about changing conditions, such as a sudden decrease in the speed of a nearby car, that might be difficult (or too quick) for a human to recognize. The U.S. Department of Transportation has been testing this technology and in February 2012 announced that it would begin taking steps to enable V2V communications in light vehicles. Although this is a great sign of things to come, it is important to recognize that both the long automotive development cycle and slow turnover rate ensure that it will still be several years before these systems become commonplace.

The Road Ahead

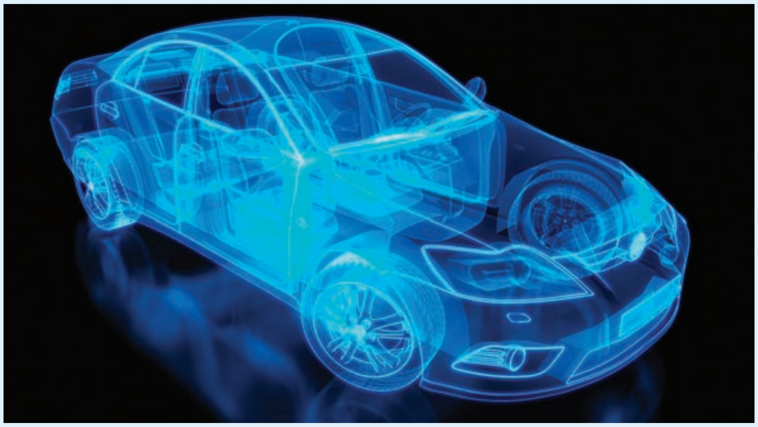
Going forward, we are excited by the prospect of the new technologies just over the horizon. As automakers (and Google) push forward with their visions of autonomous vehicles, a number of enabling technologies will become widespread. Depending on who you ask, some types of sensors are more important than others (e.g., LIDAR vs. cameras), but everyone seems to agree that massive amounts of data must be collected and processed. In some cases, nearly all of this data will be collected locally by the vehicle itself, while in other cases it will be streamed from the Cloud in large chunks. However the data arrives, it needs to be stored somewhere and will require substantial computational resources to become useful. All of this added complexity implies an increase in the number of bugs and a greater need for software updates. In order to avoid the costly overhead of visits to the service department and customer annoyance, manufacturers will need to enable over-the-air (OTA) software updates.

When we think about vehicles with massive data pipes, extensive processing power, and a more friendly application development environment, it really seems like a new wave of innovation is upon us. The key question to ask is: to what extent will manufacturers tie all of these technologies together? Furthermore, how accessible will they be to startup companies and other third-party developers? The answers to these questions are likely to have a direct impact on how rapidly we see innovation in this space. Regardless of how the pieces come together, it is safe to say that exciting changes are ahead. Q

***Gerry Hamel** is a member of the Technical Staff within IQT's Mobility practice. Prior to IQT, he worked in mobile cybersecurity, where he was heavily involved in internal R&D activities that focused on the security of mobile devices and related technologies. During this time, he also managed a team of software engineers and led the design and implementation of search and analytics platforms. Previously, he held software development roles at Jobfox and Texas Instruments. Hamel received his bachelor's and master's degrees in Electrical and Computer Engineering from Carnegie Mellon University.*

A Look Inside: Accelerating Vehicle Telematics

This issue of the *IQT Quarterly* examines recent advances in vehicle telematics, a broad technology space ranging from autonomous cars to vehicle communications and security systems. These innovative new technologies mark the beginning of a dramatic shift in the automotive industry.



Danny Shapiro of NVIDIA opens the issue with a discussion of the current and potential capabilities of in-vehicle computing. While autonomous driving is inching closer to a commercial reality, technology companies must address energy efficiency, modularity, and security implications before consumers will experience full-scale self-driving cars.

In their article, Tom Freeman and Nathan Kundtz of Kymeta cover the communications systems and related technologies that will enable smart, future-proof cars. As cars become smarter and more connected, passengers will shift their attention to new forms of data consumption. Reconfigurable antennas for mobile satellite applications, such as Kymeta's, are uniquely positioned to provide this connectivity.

Next, Paul Gray of Cohda Wireless introduces cooperative intelligent transport systems (C-ITS), a powerful new wireless sensor technology that allows vehicles to share data with other vehicles and infrastructure. With applications including intersection collision warnings and traveler information messages, C-ITS has the potential to address key transportation problems in safety, mobility, and environmental impact.

Daniel Bilar describes the threats that emerge from the use of open, networked systems in vehicles. He details attack surfaces including V2I networks, ECU connections, software, and sensors, and examines how these vulnerabilities will affect the automotive industry and its consumers.

Kyusuk Han, André Weimerskirch, and Kang G. Shin continue the dialogue on security, arguing that vehicle systems lack protection against denial-of-service attacks and external device connectivity threats. The authors' research at the University of Michigan has surfaced protocols that would protect against such attacks and establish a secure channel between vehicles and external devices.

Finally, this issue's *Tech Corner* features IQT portfolio company Weather Analytics. The rise of connected vehicles provides a unique opportunity to use weather data, such as the global, gap-free database developed by Weather Analytics, to understand and improve vehicle operations. This novel solution can optimize connected travel in areas including safety, traffic, fuel efficiency, and usage-based insurance, and is critical to reigning in the value of telematics.

Beyond the technologies presented here, there is a broad range of vehicle telematics innovation evident in startups, major commercial entities, and academia. In the coming years, these groups will continue to advance the technology capabilities in the space, while the industry's key players consider the regulatory, safety, and security concerns of connected cars. This issue of the *IQT Quarterly* is intended to provide a starting point for discussions of these technologies and issues.

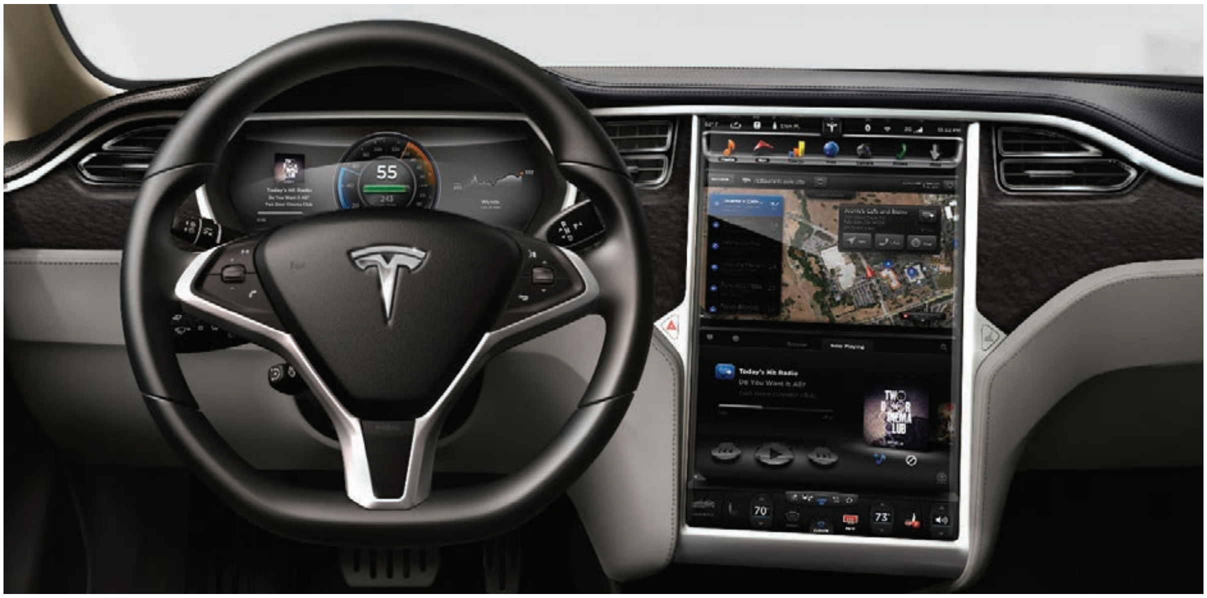


Figure 1 | Two Tegra Visual Computing Modules (VCMs) power the Tesla dashboard: one for the instrument cluster and one for the infotainment touchscreen.

FUTURE-PROOFING THE CAR

By Danny Shapiro

In the automotive industry, what was recently considered science fiction will become reality in the next few years. Technology is no longer an obstacle to bringing automotive dreams, like the self-driving car, to life. And while it is clear that there is still an enormous amount of work to do as global authorities debate the ethics, legalities, and a myriad of other implications of self-driving cars, they are now on our streets undergoing testing and development. For consumers, this automotive technology revolution will make transportation safer, more convenient, and less stressful than ever before.

Building Blocks for the Smart Car

At the heart of the drive toward the future car are the same technologies and components that made the phone smart: mobile communications, sensors, and processing technologies. Consumers now have extremely powerful computers — with location sensors, cameras, touchscreens, and wireless connectivity — in the palms of their hands, and they want the same experience inside of their cars. The challenge for automakers is not just the integration of these technologies, which has already begun, but how to do it correctly so that the car is able to keep up with the fast pace of consumer technology innovation.

The first area of the car that has experienced a technological makeover is the dashboard. In "first generation" infotainment systems that are now on the road, automakers focused on building a digital screen interface with connectivity and control capabilities for smartphones. While automakers have had mixed results in terms of the consumer success of these systems, it is clear that the digital experience is valued. The lesson learned is that the rapid pace of innovation in consumer technologies, from smartphones to tablets, raises the expectations of car buyers. While automakers have accelerated the pace of their product improvement, these cycles still average two to three years, making it very difficult to maintain up-to-date capabilities similar to what consumers experience in their homes or offices.

The answer for automakers lies in following what spurred the revolution in mobile device growth and

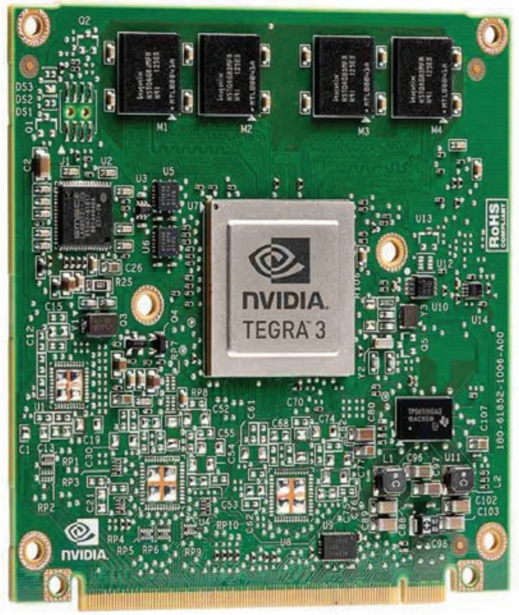


Figure 2 | The NVIDIA Tegra Visual Computing Module for the automotive industry.

innovation: building a highly-capable hardware platform with a flexible operating system that is able to adapt to future needs. This will require the adoption of advanced processing capabilities to deliver experiences such as fast touchscreen response, rich photorealistic graphics, customizable and personalized information, plus room to grow as other capabilities come online during the ownership period.

In addition to the advanced processing in the vehicle for infotainment capabilities, mobile platform developers, like Apple with iOS and Google with Android, are looking to seamlessly integrate their smartphone experience into the car. Communication to the Cloud and to mobile devices will play a valuable role in shaping the future car as consumers expect to be connected and online everywhere they go. In an effort to bring the best of the automotive and technology industries together for a solution, Audi, GM, Google, Honda, Hyundai, and NVIDIA have formed the Open Automotive Alliance (OAA), a global alliance of technology and auto industry leaders which will start bringing the Android platform to cars starting in late 2014.

This alliance will foster the use of Android in automotive applications, building off the success of the operating system in smartphones and tablets, but creating an appropriate interface for the car. The development of intuitive and simple interfaces for interacting with a connected smartphone has been a challenge for automakers, so this collaborative effort is anticipated to be a breakthrough. This organization is expected to grow significantly in the near future.

But whether it is integrating Android into the car or Apple's CarPlay interface for the iPhone, the fact that more devices are connecting to the vehicle introduces the inherent risk of security breaches. Computer viruses and hacking remain a problem today for desktop computers, so what will it take to make the car immune? To combat any malicious software potentially affecting the safety or control systems of the car, many automakers are taking a sandboxed approach, keeping the infotainment systems separate from other parts of the vehicle. Furthermore, implementing hypervisor techniques enables multiple operating systems to run simultaneously on a single system, separating them in case one has an issue.

Another area that will hugely benefit automakers in their effort to keep pace with consumer electronics is a programmable, or updatable, infotainment system. Whether consumers notice it or not, their smartphones are getting better during the ownership period by receiving over-the-air (OTA) updates. As cars become increasingly connected, OTA software updates become possible, allowing automakers to improve existing in-vehicle features and offer new ones over the course of the vehicle's life. This, of course, is expected in the consumer electronics world, but until a few years ago was totally unheard of in the automotive sector. Pioneered by Tesla Motors, OTA software updates have enabled the company to add new features while Model S cars sit in their owners' garages at night, as well as improve some vehicle parameters that may have required a costly recall if similar action was required by a traditional automaker.

Going beyond the dashboard, the area requiring the most advancement in technology, especially to achieve the vision for the self-driving car, is sensor data processing and decision-making. As more sensors — cameras, radar, laser scanners, and ultrasonic sensors — are added to the car, an incredible amount of data is being amassed every second. To process this information, massively parallel, high-performance processors are required, but they must operate in an extremely energy efficient manner. The architecture that is used for the world's fastest computers, or supercomputers, which can handle thousands of computation points every second, are needed for these automotive applications while being scaled to an appropriate size and energy efficient package.

Without these three building blocks to the future in play — intuitive user interface, seamless updates, and high-powered energy efficient performance — automakers might be stuck with trunks full of expensive desktop computers in their cars, and will never make it out of the world of research and into the mainstream.

Mobile Processors for Autonomous Driving

The seeds of full-scale autonomous driving can already be found in car models today. Various driver assistance features like pedestrian detection, lane departure warning, active parallel parking assistance, and speed limit sign recognition are incremental steps on the way to a full autonomous driving experience.

A key technology at the heart of autonomous driving is computer vision. That doesn't just mean having a lot of cameras on the car, it means having high performance and energy efficient processors that can analyze the video coming from these cameras. Sophisticated algorithms need to process the incoming information, reported to be as much as 1 gigabyte per second, in real time.

To address the increased computation needs of mobile devices (especially cars), NVIDIA recently introduced the Tegra K1 mobile processor. It packs 10 times the computing power of its predecessors and yet still operates in the same power envelope. That's essential to process all the sensor data that come into play in autonomous driving.

With a quad-core CPU and a 192-core graphics processing unit (GPU), Tegra K1 will enable camera-based, advanced driver assistance systems (ADAS) — such as pedestrian detection, blind-spot monitoring, lane-departure warning, and street sign recognition — and can also monitor driver alertness via a dashboard-mounted camera. Utilizing the same parallel processing architecture as used in high-performance computing solutions, the Tegra K1 is the first mobile supercomputing platform on the market.

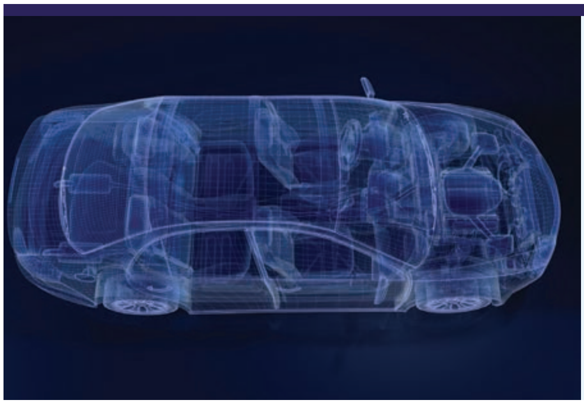
ADAS solutions currently on the market are based mainly on proprietary processors. NVIDIA Tegra K1 moves beyond this limitation by providing an open, scalable platform. The Tegra K1 processor was designed to be fully programmable; therefore, complex computer systems built upon it can be enhanced via over-the-air software updates.

In addition, this sophisticated system on a chip (SoC) can run other apps such as speech recognition, natural language processing, and object recognition algorithms interpreting in real time what is a sign, what is a car, pedestrian, dog, or ball bouncing into the road.

Automakers who are already engaged with NVIDIA and using the visual computing module (VCM) — a highly scalable computer system — for infotainment solutions can easily upgrade their in-vehicle systems with new processors due to the modular approach.

Layered on top of the Tegra processor is a suite of software libraries and algorithms that accelerate the process of creating computer vision applications for different driver assistance systems. Since these systems are software-based, automakers have the flexibility to

Figure 3 | Audi's virtual cockpit, powered by NVIDIA.



> **"The car is the ultimate mobile computer. With onboard supercomputing chips, futuristic cars of our dreams will no longer be science fiction."**
>
> — Jen-Hsun Huang, President and Chief Executive Officer, NVIDIA

update these algorithms over time, improving the overall performance and safety of the vehicle. Conversely, fixed function silicon and black boxes delivering solutions for each specific function are an expensive and ultimately dead-end route.

As the graphics on in-vehicle screens improve, personalization of this cluster is also possible. Advanced rendering capabilities on a mobile supercomputer enable in-vehicle displays to rival the visuals created by Hollywood visual effects houses and professional designers. The result is photorealistic content that looks just like real materials, such as leather, wood, carbon fiber, or brushed metal.

At the 2014 Consumer Electronics Show (CES), Audi announced a virtual digital cockpit, powered by an NVIDIA VCM. Inside the next-generation Audi TT, the virtual cockpit display can be adapted to a driver's needs, displaying the most relevant information at any time, including speedometer, tachometer, maps, menus, and music selections, helping reduce complexity and provide more customization options to its drivers.

NVIDIA has a long-standing relationship with many automakers, including Audi, Volkswagen, BMW, and Tesla. Audi was the first to deliver Google Earth and Google Street View navigation using NVIDIA technology. And during Audi's CES keynote, after one of their vehicles drove itself onto the stage, the company announced that Tegra K1 will power its piloted-driving and self-parking features currently in development.

Moving Forward with Future-Proof Cars

Given the tremendous increase in computing technology, both from hardware and software perspectives, new challenges have emerged for the automaker. Traditional supply chain models do not work when considering the need for computing platforms and complex software stacks comprised of multiple operating systems, photorealistic rendering, computer vision toolkits, and hypervisors. Only when an automaker has broken the traditional supplier model and instead created a technology partnership can the complex computing systems be developed in a cost-effective and timely manner. Integrating a supercomputer in the car is necessary to achieve the full vision for the future car, especially autonomous driving. A modular approach coupled with programmability enables these systems to rapidly evolve.

It is no secret that car makers put safety at the heart of their strategy. Moving forward, they need a technology strategy that is equally rigorous. And before long, with the right selection of supercomputing technology, we will have self-driving cars on our streets. Q

__Danny Shapiro__ is NVIDIA's Senior Director of Automotive, focusing on solutions that enable faster and better design of automobiles, as well as in-vehicle solutions for infotainment, navigation, and driver assistance. He is a 25-year veteran of the computer graphics and semiconductor industries, and has been with NVIDIA since 2009. Prior to NVIDIA, Shapiro served in marketing, business development, and engineering roles at ATI, 3Dlabs, Silicon Graphics, and Digital Equipment. He holds a B.S.E. in Electrical Engineering and Computer Science from Princeton University and an M.B.A. from the Hass School of Business at UC Berkeley. Shapiro lives in Northern California where his home solar panel system charges his electric car.

Mobile Satellite Communications for the Connected Car

By Tom Freeman and Nathan Kundtz

The reconfigurable holographic metamaterial antenna (RHMA) is an emerging technology for satellite communications. RHMAs are low-power devices that are flat, thin, and lightweight. Moreover, they achieve active electronic scanning without any mechanical moving parts. All of these physical attributes and practical considerations make the RHMA ideal for mobile satellite applications (automobiles, aircraft, trains, and ships). To operate in these rapidly and dynamically changing environments, the antenna must be software-driven, reliable, and able to scan quickly. RHMAs will help usher in a very different world in the near-term future:

Running late for a meeting, Ryan pulls his smartphone from his pocket, opens his Nagoya Motors application, and summons his car. He is greeted by his virtual driver, Mikala, who knows him well. Ryan tells her that he needs to go to "that same company we went to last Friday." Mikala disambiguates destinations through a cooperative conversation and finally figures out it's the company they went to last Thursday. Ryan sinks into his Herman Miller chair at his desk in the car, watches the various displays and monitors around his desk, tweaks his video for the upcoming presentation, watches real-time TV for a market update, and stays a couple of steps ahead in a networked multiplayer simulation. He makes a video clip of himself describing some changes he wants in his presentation and sends it to his assistant.

As Ryan works, Mikala detects that a new release of high-density maps for this particular route were prepositioned in the on-board repository last hour and she updates the navigation system. Mikala also understands the over-the-horizon energy requirements based on their destination and refueling opportunities near there, so she decides to stay all electric and not click in the petrol-based system.

While Ryan rehearses his presentation in his cab, Mikala detects a possible security probe and prioritizes a patch for the breaking system that promises to neutralize the threat. Mikala drops Ryan at the curb; Ryan banters with her that he's going in and getting out. Mikala wishes Ryan the best of luck, proceeds to evaluate his health vitals, and finds somewhere to hover until recalled.

Steerable, flat-panel antennas for satellite data connectivity are one of the components that enable this vision of the future. RHMAs enable wide-angle, all-electronic beam steering from PCB-like surfaces that can be manufactured using mature and affordable LCD manufacturing infrastructure.

The reconfigurability is achieved through the use of a standard PCB-like circuit board composed of several thousand sub-wavelength resonators (see Figure 1) that can be individually tuned. This PCB-like board is attached to a conventional feed structure. Thus, as the RF energy propagates through the system, individual tunable elements can be activated (i.e., turned "on") to scatter a portion of this RF energy out of the guided wave. It is the pattern of activated tunable elements that determines the shape and direction of the radiated

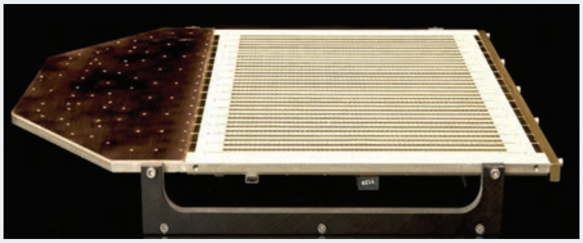


Figure 1 | The reconfigurability is achieved through the use of a standard PCB-like circuit board composed of several thousand sub-wavelength resonators that can be individually tuned.

energy through the formation of a reconfigurable grating. Changing the pattern of activated elements changes the shape and direction of the beam. The net result is an antenna with the dynamic performance of a phased array, but without the need for phase shifters and related amplifiers.

RHMA technologies are bringing unprecedented data rates to the world of networked and connected cars. What is significant and different about RHMAs is that until now, vast data rates were capable by satellite to a fixed platform inexpensively, or available to mobile platforms provided you had the enormous amounts of money, space, and energy required for phased array antennas. But now the RHMA emergence is closing this gap. The holographic metamaterial "virtually invisible" antenna is a technology that will dramatically increase consumer usage of satellite capacity by providing a means of economically connecting satellites to mobile platforms at speed.

By coupling next-generation satellite technology with pre-positioned content storage, RHMAs can offer higher performance and lower costs than terrestrial carrier networks to vehicles. By constantly raining down content and refreshing it, content is there as quickly as the consumer can click.

An important aspect of this connected car strategy is that RHMA-connected vehicles can receive, while moving at speed, emergency maps, instructions, weather conditions, and directions to safety independent of infrastructure destruction caused by man-made or natural disasters. With a small return path, telematics data can tell emergency services on what roads traffic is moving and where it is stopped. The car becomes the network and the network becomes part of the "eyes" of emergency services.

Satellite Solution Rationale

Conventional connectivity solutions to the car, such as LTE, are expensive, slow, highly balkanized, and do not scale effectively. The introduction of new connectivity technologies can dramatically improve this situation by bringing high-speed satellite solutions into the car. Historically, these solutions were inaccessible in cars because of their cost, size, reliability, power requirements, and aesthetic impact.

Terrestrial Spectrum is Limited and Congested

For the first time, RHMAs' breakthrough mobile services are possible thanks to effective access to high-throughput, high-frequency satellite bandwidth that can have low, medium, halo, and geosynchronous orbits. Connectivity at such high frequencies (>3 GHz) was historically unattainable in automobiles because of the need for directional antennas (typically a reflector or "dish" antenna). RHMA technology unlocks satellite capacity in the 12 GHz and 20 GHz bands, dramatically increasing data rates and significantly reducing costs.

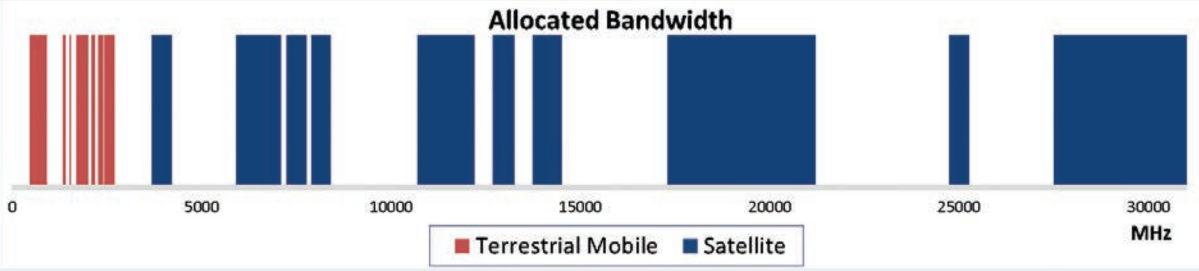


Figure 2 | Terrestrial bandwidth available for services such as LTE in contrast to satellite bandwidth available globally. While the LTE band is small and plagued with significant interference and fragmentation problems, the satellite bands have 10-100 times the capacity and can be scaled to meet the needs of the customer.[2]

There is limited terrestrial bandwidth allocated on the FCC spectrum, which includes bands for LTE as well as other mobile data plans and point-to-point connections. Mobile data consumption is growing rapidly: the A.T. Kearney 2013 *Mobile Economy* report discusses the massive growth in mobile broadband connections. Mobile broadband connections are expected to grow from 1.6 billion in 2012 to 5.1 billion in 2017, representing a 26 percent CAGR, all of which are competing for limited terrestrial bandwidth.[1] LTE/4G connections will account for 1 in 5 mobile broadband connections in 2017 versus 1 in 25 connections in 2012.[3] Networks already have trouble dealing with the saturation of LTE devices in big cities[4] — this will only get worse as more and more subscribers come online or switch to LTE/4G, and the problem will extend beyond cities. Imagine every car getting data-intensive software, firmware, and mapping updates in a world where it can be difficult to access social media in a crowded bus or stadium. Not only is vast new spectrum now leveraged, but new orbits, such as low Earth orbits (LEO) and middle Earth orbits (MEO) can be exploited.

Software and Firmware Over-the-Air (SOTA & FOTA) Updates

In addition to significantly improving throughput and reducing data delivery costs, RHMAs offer another significant advantage: no need for physical vehicle recalls and service visits to install software updates and patches. This dramatically reduces costs, helps ensure universal adoption, and prepares vehicles for the future data requirements into and out of the autonomous, and eventually networked, car. The service also provides a "mini-cloud" of infotainment and telematics content in the car for instant access, improving both driver safety and enjoyment. One major automaker estimates to the authors that 80 percent of recalls are software related.

Telematics Applications and Driver Safety Updates

1. **Maps and navigation:** RHMAs eliminate dealer visits and CD-ROM/USB manual updates to the map library. Real-time traffic updates and over-the-horizon navigation and road conditions can be delivered.

2. **Weather:** Regular weather updates, including severe weather warnings or adverse driving conditions advisories, can be delivered to the vehicle.

3. **Alerts:** Important alerts including AMBER, natural disasters, national security, and other safety alerts have a quick path into vehicles in the affected geographic regions.

Infotainment/Strategic Information

News, music, video, strategic information, and other media content can be delivered to relevant vehicles efficiently and cost-effectively. This type of content includes subscriptions, pay-per-view, and streaming media that can be aggregated and distributed on a regionally-specific basis.

Location-Based Services & Data Output

The return path enables the collection of data and location-aware or user-requested content customization. This creates opportunities for location-based assistance. Fleet management solutions and other data rich applications can take advantage of location and situational awareness.

7 GB OF MAP FILE UPDATES

Transmission Type	Transmission Speed	Transmission Time	
High Throughput Satellite (High)	1 Gbp/s	< 1 min.	High-End RHMA Solution
High Throughput Satellites (Mid)	**100 Mbp/s**	**9 min. 55 sec.**	**Target RHMA Solution**
High Throughput Satellite (Low)	30 Mbp/s	30 min.	Low-End RHMA Solution
LTE (Varies by Network & Location)	10 Mbp/s	1 hr. 30 min.	
3G	2 Mbp/s	7 hrs. 35 min.	
Sirius XM	125 Kbp/s	150+ hrs.	

Figure 3 | One minute compared with 150+ hours to replace a VW 7 GB navigation database shows the capacity and performance of RHMAs.

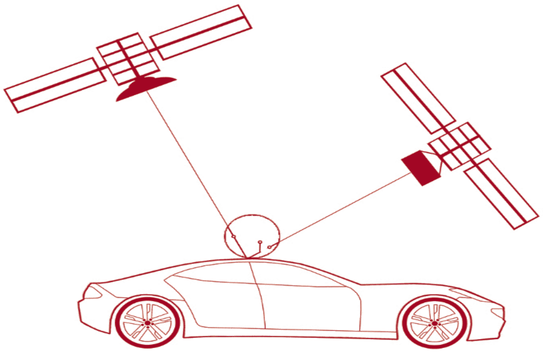


Figure 4 | Kymeta's RHMA offers the unique ability to switch dynamically between satellite constellations, operators, and bands. Content is received by a universal modem, independent of any particular satellite constellation. The universal modem can be redirected at will to different constellations for strategic, content, or emergency purposes.

As cars and fleets become more autonomous and networked, they will require more data for both the safety and operation of the vehicle, and for the informing of passengers. RMHAs enable instant updates of operating systems, firmware, and applications to enhance or defend complex systems.

Toyota, UIEvolution, and Kymeta Demonstration

Kymeta provided an early stage demonstration of an RHMA solution at CES 2014 in partnership with Toyota and UIEvolution, showing that car companies can move beyond the conventional connectivity paradigm to deliver large amounts of data cost-effectively. Kymeta's RHMA hardware and connectivity solution was paired with technology and applications developed by UIEvolution, demonstrating that 1) this data could be accessed using existing Toyota head unit and infotainment devices with no change to the current hardware form, fit, or function; and 2) content stored on the in-car Kymeta data storage device ("silver box") could be accessed by existing head units and commercial applications.

Looking Forward

As cars move from operator controlled vehicles to passenger moving machines, the time in the car will take on new value, driving new forms of data consumption and habits. The self-driving car will open the door to the living room and/or office on wheels. How that office will be serviced for connectivity is a problem Kymeta is uniquely positioned to solve. Q

__Tom Freeman__ is Senior Vice President for Land Mobile at Kymeta Corporation, where his focus is delivering content to connected mobile platforms such as the connected car. Freeman is a co-founder of VoiceBox Technologies, and he founded SPLAT.Tv (Songs Places Locations and Things), which created over-the-top and IPTV applications that leveraged broadcast awareness to monetize studios' content. Freeman is a recognized leader in the connected car industry, with experience delivering safety, security, and infotainment system solutions.

__Nathan Kundtz__ is a founder, Executive Vice President, and Chief Technology Officer of Kymeta Corporation. Kundtz is an inventor and innovator in the area of metamaterials and microwave devices. His work at Duke University in this field is highly cited as it focused on the development of new design techniques, such as transformation optics, to meet real-world needs. His work in metamaterials at Duke led to his recruitment by Intellectual Ventures in Bellevue, WA, where he pioneered the application of metamaterials technology in electronic beamforming applications. The success of this technology at Intellectual Ventures ultimately led to the spin-out of Kymeta Corporation in August 2012.

REFERENCES

[1] Page, Mark et al. "The Mobile Economy 2013." A.T. Kearney. 2013. http://www.atkearney.com/documents/10192/760890/The_Mobile_[1] Economy_2013.pdf.

[2] Federal Communications Commission. "Spectrum Dashboard." Retrieved June 2, 2014, from http://reboot.fcc.gov/spectrumdashboard/searchMap.seam.

[3] Page, Mark et al. "The Mobile Economy 2013." A.T. Kearney. 2013. http://www.atkearney.com/documents/10192/760890/The_Mobile_[1] Economy_2013.pdf.

[4] Albanesius, Chloe. November 13, 2013. Verizon's 4G LTE Network Struggling in Big Cities. *PC Mag.* http://www.pcmag.com/article2/0,2817,2427077,00.asp.

CONNECTING SMART CARS AND INFRASTRUCTURE IN A WIRELESS SENSOR NETWORK

By Paul Gray

Cars are undoubtedly safer now than ever, as evidenced by the steady decline of road fatalities. However, the number of injuries is actually increasing; passive safety technologies such as seat belts and airbags have simply made accidents more survivable. It seems obvious that what is needed are ways of avoiding the accidents in the first place. Meanwhile, traffic congestion, and its resulting environmental impact, continues to be a growing problem in cities around the globe. One simple communications technology has the potential to address all of these issues.

Transportation Challenges

Governments around the world are concerned about the societal costs of road transport. These costs are often categorized as safety, mobility, and environmental concerns.

First and foremost is safety. In Europe, there were 38,000 fatalities and 1.7 million injuries in 2008. Human error was a factor in 93 percent of accidents. In the U.S., there were 37,000 fatalities and 5.8 million accidents in 2008, and road accidents were the leading cause of death for people between the ages of 4 to 34. The direct cost of traffic accidents was $230 billion.

Another significant cost of transportation is congestion, resulting in reduced mobility. In Europe, 10 percent of the road network is congested daily and a staggering one percent of GDP is lost to congestion annually. In the U.S., congestion costs the economy $87 billion annually, the result of 4.2 billion lost hours.

Closely linked to congestion is the impact of transport systems on the environment. In the U.S., transportation is the single largest contributor of greenhouse gas emissions, and 2.8 billion gallons of fuel are wasted annually due to congestion.[2]

Cooperative ITS

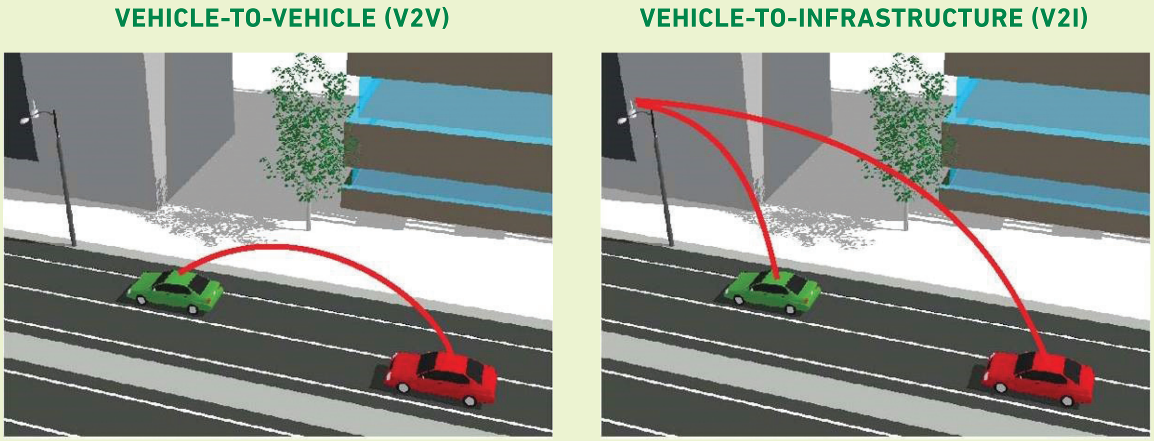
Cooperative intelligent transport systems (C-ITS) use both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications — collectively called V2X communications — to enable cooperation between vehicles and road infrastructure to improve safety, mobility, and the environment. The goal of C-ITS is to create wireless communications links between smart vehicles and between vehicles and "smart roads" in order to allow them to “talk” to each other, avoid accidents, reduce congestion, and improve efficiency.

A major point of focus for C-ITS in the U.S. comes from the Department of Transportation’s ITS Joint Program Office. In Europe, there are a number of Framework 6 and 7 projects (the EU's main instruments for funding research to respond to employment needs, competitiveness, and quality of life) which are focused on C-ITS: SafeSpot, COOPERS, CVIS, Drive-C2X, and simTD, to name only the major transnational projects. Other C-ITS programs are in place in Australia, Korea, and Japan.

Safer, Smarter, Greener

C-ITS is an emerging market that will make road transportation safer, smarter, and greener. The Department of Transportation estimates that V2V communications can address 79 percent of all accidents, while V2I communications can address 26 percent of all accidents. Combined, predictions are that C-ITS systems could provide warnings in up to 81 percent of all accidents.[3]

Both the U.S. and Europe have already released valuable radio spectrum at 5.9 GHz that is dedicated for C-ITS.



VEHICLE-TO-VEHICLE (V2V)

VEHICLE-TO-INFRASTRUCTURE (V2I)

Robust V2V connectivity supporting safety applications:

- Forward collision warning
- Intersection collision warning
- Emergency electronic brake light
- Do not pass warning
- Intersection movement assist

V2I broadband connectivity supporting safety and mobility applications:

- Curve speed warning
- Red light violation warning
- Security certificate updates
- Traffic probe snapshot
- Traveler information messages

Figure 1 | V2V and V2I applications.

In the U.S., a total of 75 MHz in the 5.9 GHz has been allocated, while in Europe an initial 30 MHz has been allocated with a planned roadmap for 70 MHz. In both regions, the spectrum is aligned. The U.S. ITS program is focused on collecting the data necessary for the National Highway Traffic Safety Administration (NHTSA) to regulate use of C-ITS. The European Commission has mandated that European Standards Organizations must develop C-ITS standards as part of its ITS Action Plan and ITS Directive. Major trials of C-ITS are underway around the world. In Europe, a consortium of 12 automakers have signed a memorandum of understanding (MoU) committing to deployment of C-ITS in production vehicles commencing in 2015.

The foundation standards for C-ITS are the same in both the U.S. and Europe and have already been published.

Vehicle-to-vehicle applications for C-ITS include the following:

- **Forward collision warning:** Warning of collision hazards ahead of the vehicle, such as a slow or stopped vehicle in the lane ahead, even on curved roads.
- **Intersection collision warning:** Warning of side-collision hazards as vehicles approach an intersection, even in blind intersections.
- **Emergency electronic brake light:** Warning of a vehicle braking ahead, even when the vehicle is obscured by an intervening truck.
- **Do not pass warning:** Warning of a collision hazard during overtaking maneuvers, even on curves and hill crests.
- **Intersection movement assist:** Warning of collision hazards for stopped vehicles about to enter an intersection.

Vehicle-to-infrastructure applications for C-ITS include the following:

- **Curve speed warning:** When a vehicle passes a roadside unit it is sent a Local Dynamic Map (LDM) containing information about nearby dangerous curves. Subsequently, if the vehicle is approaching one of these curves too fast, a warning is generated.
- **Red light warning violation:** Signal phase and timing (SPaT) information is sent from traffic lights to approaching vehicles, and a warning is provided if the vehicle is about to violate a red light.
- **Security certificate updates:** Every message transmitted in C-ITS includes a signature using public key cryptography, with a certificate issued by a trusted authority. This ensures that only authorized messages are acted upon. Certificates only have a limited lifetime, and new certificates can be downloaded from roadside units.

- **Traffic probe snapshots:** As vehicles travel, they can take regular snapshots of vehicle speed and traffic conditions. These snapshots can be uploaded whenever the vehicle is in range of a roadside unit. This turns vehicles into mobile sensors and gives a traffic management center a near-real-time view of traffic conditions.
- **Traveler information messages:** Information currently provided by roadside signs, such as variable message signs or variable speed signs, can be brought into the vehicle.

Wireless Sensors

The access layer in C-ITS systems is IEEE 802.11p, a variant of the ubiquitous WiFi standards. This often leads to the misapprehension that C-ITS is a communications system. While communication is certainly possible with these systems, they are, in essence, wireless sensor systems. In order to deliver the promised safety benefits of C-ITS, these systems must be high-availability, low-latency (HALL) systems. The changes introduced into IEEE 802.11p were to use a lower bandwidth making the signals more robust (high availability), and to eliminate the need for handshaking before packets could be exchanged (low latency).

For example, as two vehicles approach each other in the V2V intersection collision warning application, they would exchange sensor data such as position, speed, heading, steering wheel angle, 3D acceleration, and brake status. Such information is shared in a single packet broadcast to surrounding vehicles ten times per second, allowing each vehicle to assess threats from other vehicles based on sensors located in the other vehicles.

As we move towards automated driving, and even autonomous driving, these C-ITS wireless sensors will be increasingly important. Automated driving depends on the fusion of several sensors, such as radar, optical, and LIDAR. However, all of these sensors are line-of-sight sensors and cannot outperform human senses (assuming the driver is looking in the correct direction). The addition of C-ITS wireless sensors extends the sensor horizon beyond human senses, allowing the sensing of threats around corners, over the crests of hills, and through trucks.

LTE and 3G cellular systems are often cited as viable alternate access layers to IEEE 802.11p for C-ITS. However, these are communications systems, not wireless sensor systems. The latency of these cell-based systems is just too high — all messages must be passed from one car to a distant base station, and then from the base station to the other car. While it may be true that LTE Direct could reduce this latency, work on LTE Direct is in its infancy. On the other hand, IEEE 802.11p standards have been published for several years, and field trials of C-ITS based on IEEE 802.11p have been completed.

Naturally, these C-ITS systems need to be robust and reliable in order to achieve the high availability requirement. While it is possible to repurpose consumer-grade WiFi chips for C-ITS, these chips were designed for home and office wireless environments, not outdoor,

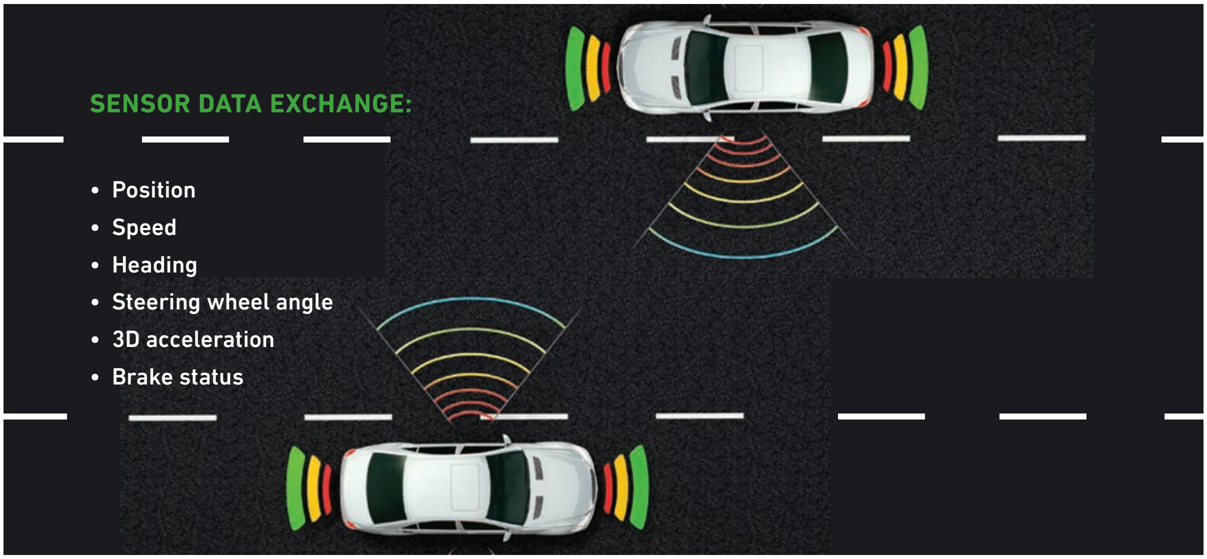


Figure 2 | Sensor data exchange between two approaching cars equipped with a V2V intersection collision warning application.

mobile automotive environments. As such, there are significant performance differences between consumer-grade WiFi chips and automotive-grade C-ITS chips. This difference has resulted in the establishment of minimum performance requirements for C-ITS systems.

Current Status

Trials of C-ITS systems have been conducted in both Europe and the U.S. In Europe, the major trials have been simTD and Drive-C2X, where 500 vehicles fitted with C-ITS have been tested on the road. The U.S. is currently home to the largest C-ITS trial to date, where 2,800 vehicles have been on the road for 18 months in Ann Arbor, Michigan.

In January 2014, NHTSA announced that it will start taking steps to enable V2V communication technology for light vehicles. This is expected to result in a mandate of C-ITS technology in all new light vehicles according to the following timeline:

- **2014 (NHTSA):** Agency decision to consider dedicated short-range communications (DSRC) rulemaking for light vehicles
- **2015 (NHTSA):** Agency decision to consider DSRC rulemaking for heavy vehicles
- **2016 (FHWA):** Development of infrastructure deployment guidance
- **2018 (State DOTs):** First traffic signals with DSRC installed
- **2020 (State DOTs):** 20 percent of traffic signals with DSRC installed

In Europe, the governments of The Netherlands, Germany, and Austria have signed an MoU for the deployment of a corridor of roadside units that will extend from The Netherlands, through Germany, and into Austria. This has been dubbed The Corridor Project and will support applications such as traveler information messages, roadworks alerts, and emergency vehicle alerts.

Meanwhile, automakers in the U.S. and Europe have begun to release Requests For Quotations (RFQ) for C-ITS systems for production vehicles. The lead automakers in this space are expected to include C-ITS systems in production vehicles beginning in 2016. Early adopters in Europe gain the selling point of cars that can use the facilities deployed by The Corridor Project, while early adopters in the U.S. are betting that a mandate will follow.

Conclusions

Cooperative intelligent transport systems based on IEEE 802.11p standards are powerful new wireless sensor systems that permit vehicles to share their sensor data with other vehicles around them. Extensive global trials of these systems have demonstrated that they can have a dramatic effect on safety, mobility, and the environment.

Furthermore, as we move towards automated and autonomous driving, C-ITS wireless sensor systems can provide valuable non-line-of-sight sensor data from around corners, over the crests of hills, and through trucks.

Dr. Paul Gray *is CEO of Cohda Wireless, a leading specialist in wireless communications for automotive safety applications. He was originally Cohda's Chief Engineer and has led the development of all of Cohda's products to date. Since becoming Cohda's CEO in 2011, Gray has also turned his focus to strategic engagements and business planning. Prior to Cohda, he was Business Manager for TrellisWare, where he led commercial activities including the development of a novel 1 Gbps turbo code chip. Previously, Gray was CTO of iCODING, a startup focused on developing and licensing IP for turbo codes.*

REFERENCES

[1] http://docbox.etsi.org/Workshop/2010/201002_ITSWORKSHOP/1_OPENINGandKEYNOTE/JAASKELAINEN_EUCooperativeMobility.pdf
[2] http://www.its.dot.gov/strategic_plan2010_2014/2010_factsheet.htm
[3] http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2010/811381.pdf

FURTHER READING

- U.S. Department of Transportation Joint Program Office. http://www.its.dot.gov/.
- SafeSpot. http://www.safespot-eu.org/.
- COOPERS. http://www.coopers-ip.eu/.
- CVIS. http://www.cvisproject.org/.
- Drive-C2X. http://www.drive-c2x.eu.
- simTD. http://www.simtd.de.

IDENTIFYING TELEMATICS THREATS

By Daniel Bilar

The telematics revolution, like other revolutions, is at its core about trade-offs. We are willing to trade hitherto closed systems for open systems and the promise of individual and collective benefits such as convenience, entertainment, performance, and predictive control. Often disregarded are less appealing aspects of this bargain, such as threats that emerge from the use of networked, open systems.

This article will delineate such threats by describing the attack surfaces of the telematics vision. These attack surfaces appear at every scale; from the vehicle-to-infrastructure networks that link vehicles to traffic control, repair, and radio networks, down to the FlexRay, MOST, LIN, and CAN networks that connect electronic control units (ECUs) in vehicles; every element in the connected car — from software code, interfaces, sensors, protocols, and control logic to the linked infrastructure — has implications for society, the economy, and culture.

The Connected Car

The connected car, like the Internet, decomposes into a network of networks, which in turn is linked to and embedded in larger vehicle-to-vehicle and vehicle-to-infrastructure networks. A modern car contains between 30-150 ECUs, which can be viewed as special-purpose communicating control devices with limited memory and power. They are grouped in separate networks in a partitioned bus topology, interconnected via gateways (see Figure 1). Common networks include CAN, LIN, MOST, FlexRay, and PSI5; these differ in bandwidth, latency, openness, and cost. For example, critical applications like the powertrain are handled by high-speed CAN networks, lesser priority "comfort" applications like door locking and seat adjustments are handled by LIN/low-speed CAN, whereas FlexRay is used for driver assistance and MOST for high bandwidth entertainment (not shown is PSI5 for passive driver assistance).

ECUs may feature Unix-like operating systems, such as telematics shown in orange in Figure 2. Some ECUs can be accessed remotely over long ranges (e.g., cellular, radio), some over shorter ranges (e.g., Bluetooth, keyless entry, or the tire pressure monitoring system), yet others require physical access (e.g., ODB-II, iPod). Figure 3 provides a stylized abstraction.

Attack Surfaces, Protocols, and Messages

The telematics channels span attack surfaces, since it is through these entry points that data gets passed to and from the vehicle's networks and onto the ECUs. ECU communication is affected via one-, two-, or multi-way protocols that exchange standardized, network-specific messages. Sent messages are received, parsed by the recipient's input parsing routine (a "recognizer"), and affect ECU actions. Such actions may include actuators or internal and external control signal generation, which often means new message generation. An attacker communicating through the attack surface/access channels is free to choose what to focus on: crafting messages to subvert protocol logic, a run-around of the input recognizer, influencing the message-dependent feedback system, or any combination thereof. Success will depend on finding realizable vulnerabilities.

Vulnerabilities

The triad of error, vulnerability, and exploit lies at the heart of conventional "hacking."* Vulnerabilities are realizable weaknesses in systems. These weaknesses are introduced at design and/or implementation time and may manifest at the code, protocol, or systemic levels. These weaknesses may — but needn't — be caused by explicit errors.[1] Sometimes vulnerabilities arise not from logic or coding errors but from violations of implicit trust assumptions. Yet another class of vulnerabilities may be induced by the aggregate interactions of individual elements. Lastly, exploits target vulnerabilities in order to interfere with normal execution and control flow. At least two of the three classes of vulnerabilities are present in the in-vehicle networks themselves, as the research over the last decade has shown. Among the more serious ones are insufficient bus protection in terms of confidentiality, integrity, availability, and non-repudiation; weak or non-existent authentication anent reflashing ECUs; protocol misuse through specially crafted messages resulting in denial-of-service attacks, network shutdown, and disconnects, in addition to "standard" protocol problems like deviation from specifications and data leakage.[2]

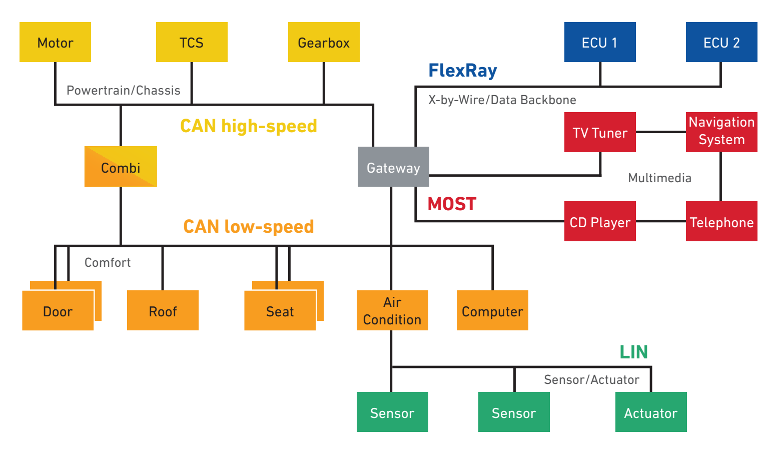


Figure 1 | Vehicle network: CAN, FlexRay, MOST, and LIN networks, interconnected by a gateway.

Exploits

As Checkoway demonstrated in 2011, the OBD-II port, Bluetooth, the cellular channel, or media devices such as a CD player may serve as access points.[3] The exploits are quite trivial: code weaknesses such as buffer overflows and design weakness such as weak PINs (see overview in Figure 5). Checkoway noted that nearly all vulnerabilities emerged at interface boundaries ("glue code") written by distinct organizations (an aspect of the "secure composition" problem, to which we will return). One may inquire as to the purpose of exploits: a payload could be deployed post-exploit that records the door locking messages on the low-speed CAN network, then proceeds to replay it at a later time, thereby unlocking the doors and finally starting the engine.[4] More sinister payloads are feasible.

In summary, attackers may read, spoof, drop, modify, flood, steal, and replay messages with relative ease. How did this state of affairs come about?

Trust Assumptions

Implicit and explicit trust assumptions are reflected in the design and implementation of any system, including the wider Internet and vehicular systems. For historic reasons, the main assumption is that participants are

* The error, vulnerability, and exploit triad is applicable across many domains, as the following 19th century legal example may illustrate: The U.S. Tariff Act of 1872 was to include a list of duty-free items: Fruit plants, tropical and semi-tropical. A government clerk duly transcribed the Act, but erroneously moved the comma: Fruit, plants tropical and semi-tropical. Shrewd businessmen argued that the law, as promulgated, exempted all tropical and semitropical plants from duty fees, resulting in a $500,000 loss to the U.S. Treasury.[5] The erroneous placement of the comma is the error. The vulnerability manifests itself as an opportunity for alternative interpretation, and the exploit is represented by taking advantage of duty-free imports of tropical and semi-tropical plants.

benign, rather than malicious. As a corollary of this trust, message (input) is trusted, code and protocols are "lean" and intended to handle quasi-random errors. Specifically, they are not designed to handle deliberate subversion and attacks.[6] In an old-fashioned, isolated "closed" car, it is not unreasonable to assume that components will play nice with one another. These trust assumptions, however, are not likely to hold true in the case of the connected car.

Secure Composition and LangSec

We mentioned glue code and secure composition. There is yet another deeper reason why it is hard to give security guarantees for composed systems, even if the components play nice. The secure composition problem can be stated thusly: can something be said about the security properties of collective system AB if individual security properties of A and B are known? It turns out that for the majority of interacting systems in use today (notable, expensive exception: NASA flight software), the answer is no; a "halting problem" is at the root of the composition problem. Secure composition requires parser computational equivalence, which is undecidable for many language classes.[7]

Specifically, a composition of communicating units must rely on computational equivalence of its input-handling routines for security (also correctness when defined). Such equivalence is undecidable for complex protocols (starting with those that need a nondeterministic pushdown automaton to recognize their input language), and therefore cannot be checked even for differing implementations of the same communication logic. Formal input verification (i.e., that input to a parser/recognizer constitutes a valid expression in an input-handler protocol's grammar), as well as verifying the semantics of input transformations, is an overlooked security aspect, and one that should be explicitly addressed in the connected car vision.

Mitigations

There are well-known approaches, some dating back decades, to identifying and fixing coding errors and unsafe functions, such as static analysis, fuzzing tools, and rigorous coding standards.[8] Recently, formal verification methods have gained some traction and high profile success. From a protocol point of view, the adoption of standard security mechanisms such as ECU

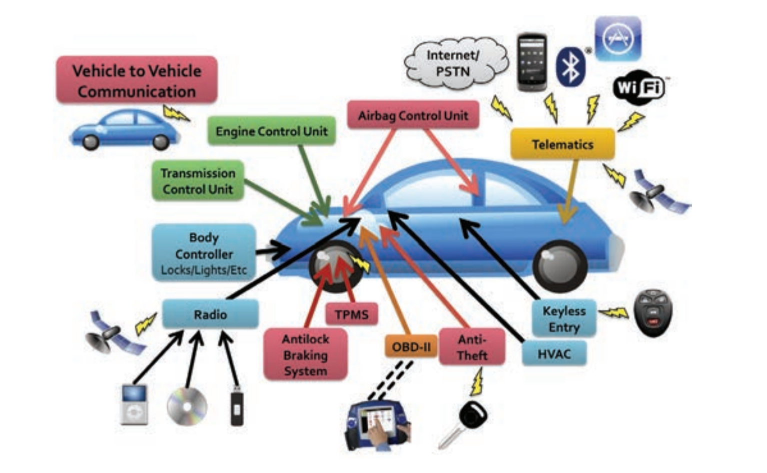


Figure 2 | ECUs grouped by functionality.[3]

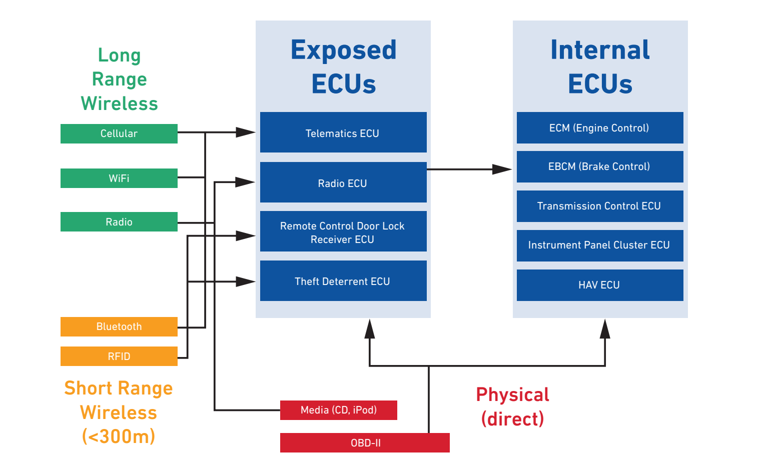


Figure 3 | Communications path/access channels into vehicle ECUs.

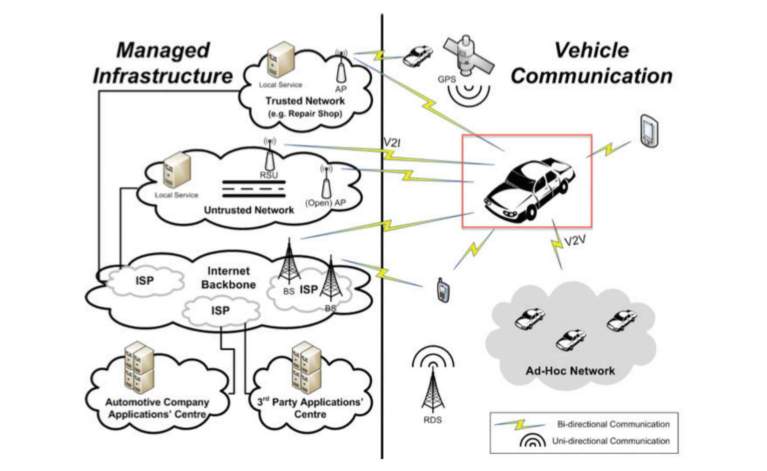

Managed Infrastructure
Local Service
AP
Trusted Network (e.g. Repair Shop)
Vehicle Communication
GPS
V2I
RSU
Local Service
(Open) AP
Untrusted Network
ISP
Internet Backbone
BS
ISP
BS
ISP
V2V
Ad-Hoc Network
Automotive Company Applications' Centre
3rd Party Applications' Centre
RDS
Bi-directional Communication
Uni-directional Communication

Figure 4 | Connected car infrastructure: vehicle, V2V, and V2I networks.[9]

Vulnerability Class	Channel	Implemented Capability
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port
Indirect physical	CD	CD-based firmware update
	CD	Special song (WMA)
	PassThru	WiFi or wired control connection to advertised PassThru devices
	PassThru	WiFi or wired shell injection
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)

Figure 5 | Access channels, vulnerabilities, and exploits.[3]

message encryption, MAC integrity/authentication, as well as hardware solutions such as Trusted Platform Module would vitiate large swaths of the "low-hanging fruit" attacks.[10, 11] However, car companies are sensitive to tangible costs that affect the bottom line (such as additional hardware) and the performance of the vehicle (such as checks and protocol overhead). For the secure composition problem, a principled approach has been proposed, called the minimal computational power principle. The idea is to restrict the language of messages exchanged by system components to a necessary minimum of computational power required for their recognition, ideally to a language class (e.g., regular expressions) for which the parser equivalence problem is decidable.

Systemic Computer Security Issues

So far, we have focused on single vehicle issues. What about the larger embedding networks, such as traffic systems? We would like to be able to say something reassuring about the collective behavior of quasi-autonomous vehicles acting as physical agents/sensors in traffic and other closed loop systems, such as: it's safe, useful, and moral.

Aggregate behavior of simple agents was studied in the past (e.g., Bell Labs' Core War in the 1960s, Conway's Life in the 1970s, and Koza's LISP programs in the 1990s). These remained interesting curiosities with no real-world ramifications. In 2012, Johnson studied phenomenological "signatures" of interacting autonomous computer agents in real-world dynamic (trading) systems. The agents were making autonomous decisions based on global/local market signals. An all-machine time regime could be identified, characterized by frequent "black swan" events with ultrafast durations (<650 ms for crashes, <950 ms for spikes), causing 18,000 extreme price change events.[12] Is it possible for similar collective pathological behavior to arise in traffic systems made up of autonomous vehicles? Phenomenological signatures may serve as collective system health indicators. For instance, it is possible to tell whether certain systems (exhibiting strategic interactions of self-interested agents) are in a Nash equilibrium based on such signatures.[13]

Assuming optimistically that safety guarantees can be given, will the sensor network promise pay off in terms of value? It seems strange to suppose otherwise: more data must enable better decisions. However, optimization problems are different for systems in high dimensional parameter space. The vastness of such systems overwhelms "rational learning" algorithms, making them effectively no better than random meanderings.[14] More data may not necessarily translate into making better decisions.

Lastly, far-reaching consequences of the telematics revolution need to be discussed with all stakeholders with some sense of urgency. Self-driving cars may make vast swaths of blue- and white-collar workers obsolete and affect changes in social processes, as experiences with driverless trucks and trains in Australian mines have shown.[15]

The reimagining and reengineering of our vehicular infrastructure affects our economies, societies, cities, and values.[16] From a manufacturing perspective, self-driving cars may affect vehicular design decisions such as windshield composition and strength, suspension, cargo space, and weight; again with economic and social ramifications up– and downstream.[17] Who is responsible for accidents in such traffic systems? Autonomous decision chains will make it necessary to revisit long-settled fundamental questions of product legal liability and moral agency.[18, 19] It may not be all bad: as self-driving car inventor Sebastian Thrun noted, the big losers could be the trial lawyers.

__Dr. Daniel Bilar__ is Director of Research and Senior Principal Scientist for an R&D company specializing in cybersecurity supporting the U.S. commercial, defense, and Intelligence communities. His areas of specialization include complex malware, moving target defenses, information operations, and quantitative compositional risk analysis and management of systems. He was one of seven founding members of the Institute for Security Studies at Dartmouth, where he conducted technological counter-terrorism research for the Department of Justice and the Department of Homeland Security. He is a recognized expert in U.S. Federal Court on computer security, programming, risk profiling, code logs, and general forensics. Bilar holds a Ph.D. in Engineering Sciences from Dartmouth, a M.Eng. in Operations Research and Industrial Engineering from Cornell, and a B.A. in Computer Science from Brown.

REFERENCES

[1] K. Tsipenyuk, B. Chess and G. McGraw. "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors." *IEEE Security and Privacy* 3:6. Nov 2005. pp. 81-84. https://cwe.mitre.org/documents/sources/SevenPerniciousKingdoms.pdf.

[2] A. Lang, et al. "Future Perspectives: The Car and Its IP-Address — A Potential Safety and Security Risk Assessment." *SAFECOMP.* Sept. 2007. pp. 40–53.

[3] S. Checkoway, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." *USENIX.* August 2011. http://www.autosec.org/pubs/cars-usenixsec2011.pdf.

[4] D. Nilsson and U. Larson. "Simulated Attacks on CAN Buses: Vehicle Virus." *AsiaCSN.* 2008. pp. 66–72. http://portal.acm.org/citation.cfm?id=1713277.1713292.

[5] "Forty-Third Congress; First Session Feb. 20." *New York Times.* February 21, 1874. http://query.nytimes.com/mem/archive-free/pdf?res=9902EFD8173BEF34BC4951DFB466838F669FDE.

[6] D. Bilar. "Degradation and Subversion through Subsystem Attacks." *IEEE Security & Privacy* 8:4. July-Aug. 2010. pp. 70-73. http://docdroid.net/agqk.

[7] L. Sassaman et al. "Security Applications of Formal Language Theory." *IEEE Systems Journal* 7:3. Sept. 2013. pp. 489-500. http://langsec.org/papers/langsec-tr.pdf.

[8] J. Holzmann, "The Power of 10: Rules for Developing Safety- Critical Code", *Computer* 39:6, June 2006, pp. 95-99 http://spinroot.com/gerard/pdf/Power_of_Ten.pdf.

[9] P. Kleberger, A. Javaheri, T. Olovsson, and E. Jonsson. "A Framework for Assessing the Security of the Connected Car Infrastructure." *ICSNC 2011.* IARIA. Oct. 2011. pp. 236–241. http://www.thinkmind.org/download.php?articleid=icsnc_2011_10_30_20229.

[10] M. Wolf and T. Gendrullis. "Design, Implementation, and Evaluation of a Vehicular Hardware Security Module." *ICISAC.* Nov 2011. http://evita-project.org/Publications/WG11.pdf.

[11] P. Kleberger, T. Olovsson, and E. Jonsson. "An In-Depth Analysis of the Security of the Connected Repair Shop." *ICSNC 2012.* IARIA. Nov. 2012. pp. 99–107. http://www.thinkmind.org/download.php?articleid=icsnc_2012_5_10_20167.

[12] N. Johnson et al. "Abrupt Rise of New Machine Ecology Beyond Human Response Time." *Nature Scientific Reports.* September 2013. http://dx.doi.org/10.1038/srep02627.

[13] Y. Vorobeychik et al. "Noncooperatively Optimized Tolerance: Decentralized Strategic Optimization in Complex Systems." *Phys. Review Letters.* 107 (10). 2011. http://link.aps.org/doi/10.1103/PhysRevLett.107.108702.

[14] T. Galla and J. Farmer. "Complex Dynamics in Learning Complicated Games." *PNAS.* 110 (4). 2013. http://www.pnas.org/content/110/4/1232.full.pdf+html.

[15] K. McNab et al. "Exploring the Social Dimensions of Autonomous and Remote Operation Mining." *Final Cluster Report.* University of Queensland. Feb. 2013. https://www.csrm.uq.edu.au/publications/exploring-the-social-dimensions-of-autonomous-and-remote-operation-mining-applying-social-license-in-design.

[16] P. Ross. "Driverless Cars: Optional by 2024, Mandatory by 2044." *IEEE Spectrum.* May 2014 (accessed June 4th, 2014). http://spectrum.ieee.org/transportation/advanced-cars/driverless-cars-optional-by-2024-mandatory-by-2044/.

[17] A. Madrigal. "When 'Driver' Goes the Way of 'Computer.'" *Atlantic Monthly.* May 2014. (accessed May 28, 2014). http://www.theatlantic.com/technology/archive/2014/05/when-driver-goes-the-way-of-computer/371692/.

[18] J. Villasenor. "Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation." *Report,* Brookings Institute. April 2014. http://www.brookings.edu/~/media/research/files/papers/2014/04/products%20liability%20driverless%20cars%20villasenor/products_liability_and_driverless_cars.pdf.

[19] R. Arkin et al. "Moral Decision Making in Autonomous Systems: Enforcement, Moral Emotions, Dignity, Trust, and Deception." *Proceedings of the IEEE.* 100.3. 2012. pp. 571-589. https://smartech.gatech.edu/bitstream/handle/1853/40769/IEEE-ethicsv17.pdf?sequence=1.

Automotive Cybersecurity for In-Vehicle Communication

By Kyusuk Han, André Weimerskirch, and Kang G. Shin

Automotive cybersecurity issues have emerged as information technologies are increasingly deployed in modern vehicles, and security researchers have already demonstrated the associated threats and risks. Although many security protocols have been proposed, they have not considered the threats posed by denial-of-service (DoS) attacks and external connectivity vulnerabilities. To alleviate this problem, we've proposed a new, secure in-vehicle communication protocol, called "ID-Anonymization for CAN (IA-CAN)." This protocol can protect against DoS attacks as well as provide a secure channel between in-vehicle components and external devices for advanced connected vehicle applications.

Vehicle Connectivity and Cybersecurity Risks

Modern cars are equipped with an average of 70 electronic control units (ECUs) that provide advanced functionality in the vehicle. These ECUs are internally connected via serial buses and communicate using a de facto standard protocol called the Controller Area Network (CAN). Recent innovations in automobile communication technology include vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) short-range communication, as well as vehicle-to-Internet communication via an embedded modem or Bluetooth-paired cell phone. Connected vehicle technology also includes connectivity to external devices such as smartphones and tablet PCs. One example is Ford Motors' OpenXC that directly extracts rich data from the vehicle (OBD-II port) and transmits the data to Android devices through a vehicle interface (VI) as depicted in Figure 1.

As vehicle connectivity becomes more common, new security risks emerge. For example, RiskIQ claimed that malicious mobile apps are becoming more prevalent, and in 2013, 12.7 percent of all Google Play apps were malicious.[1] The likelihood of successful automotive attacks increases with the number of Bluetooth-enabled vehicles that use paired smartphones, which in turn can be used as attack paths. Current vehicle systems are dreadfully vulnerable against these threats due to the lack of security considerations in the architectural design.

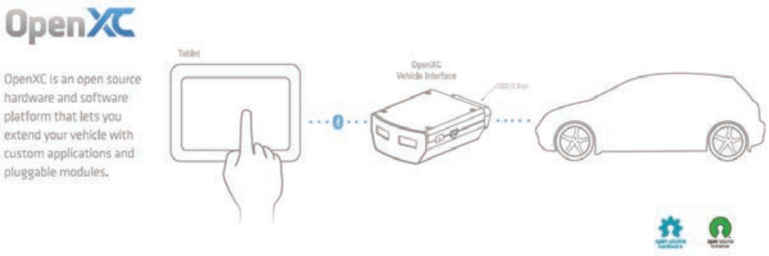

OpenXC
OpenXC is an open source hardware and software platform that lets you extend your vehicle with custom applications and pluggable modules.
Tablet
OpenXC Vehicle Interface
OBD II Port

Figure 1 | Ford Motors' OpenXC (http://openxcplatform.com/).

When CAN originally became the de facto automotive standard in the 1980s, design choices were greatly influenced by strict constraints such as low cost and low network latency, while CAN security was barely considered. CAN is still used today, but the automotive landscape has drastically changed, with cars being connected through wireless interfaces and electronics being increasingly important. Security researchers have already reported the weaknesses of CAN in today's vehicles. For example, in 2010, Koscher et al. argued that CAN is insecure and vulnerable to attacks, attributing the following major drawbacks of the CAN architecture:

- There is no provision for authenticating the sender and the receiver of a frame.
- A CAN frame has no authentication field.
- The payload field in a CAN frame provides only up to 8 bytes of data.
- Current ECUs have too limited computational capability to perform a significant number of cryptographic operations.

In practice, vulnerabilities in current automotive networks are demonstrated by presenting various attack scenarios, e.g., disabling brakes, turning off headlights, and taking over steering (for cars equipped with parking assistant).[2,3] Note that other protocols, such as FlexRay, have also been introduced and deployed without addressing security.

Unfortunately, it is difficult to overhaul the entire design of this architecture to support security mechanisms due to cost. Therefore, adding security functions without compromising the current standard becomes the important industry requirement.

An attacker's behavior can be categorized into four types: ***interception, injection, modification,*** and ***interruption***.[4] Attack routes are categorized into physical access and remote access. While most practical and probable attacks are through remote access (e.g., compromising the vehicle interface in Figure 1), we digest possible attack scenarios below.[5] Table 1 shows more details.

1. **Extract keys**: After compromising an entity (the user's external device or the gateway [vehicle interface in Figure 1]), the attacker may try to extract the secret information from a user's device or from the gateway.
2. **Impersonating a user's device or a gateway**: An attacker's device may try to impersonate a user's device or a gateway.
3. **Fraudulent requests from a compromised user's device**: An attacker may compromise a user's device and then send invalid requests to the ECUs.
4. **Fraudulent requests from a compromised gateway**: An attacker may try to compromise the gateway through wired or wireless communications. He or she may then send malicious commands or codes to the gateway to read unauthorized vehicle information or to write control commands to the CAN.

State of the Art: Secure CAN

There have been several efforts to enhance the communication security in extremely constrained environments, where only up to 8 bytes are allowed for data transmission and ECUs' capabilities are limited.

- Nilsson et al. proposed to use the CRC field instead of consuming the data field in 2008. They link multiple CAN messages and use multiple 16-bit CRC fields to contain 64 bits of CBC-MAC.[6]
- Szilagyi and Koopman proposed a multicast authentication protocol by validating truncated MACs across multiple packets in 2010.[7]
- Schweppe et al. proposed a truncated MAC model that uses 4 bytes for message authentication to fit in the data field in 2011.[8]
- Groza and Murvay proposed broadcast authentication by deploying the TESLA (timed efficient stream loss-tolerant authentication) model intended for wireless sensor networks in 2012.[9]
- Hartkopp et al. proposed the flexible model that supports various conditions with time synchronization in 2012.[10]

The two glaring drawbacks of these approaches in the real-time system are: (1) receivers first accept all incoming frames irrespective of their validity; and (2) receivers need to do cryptographic computations to verify the validity of all frames, which inevitably incurs significant additional delay and becomes vulnerable to DoS attacks.

ID-Anonymization for Secure CAN

To overcome these drawbacks, we developed a concept of ID Anonymization for CAN (IA-CAN), where the frame ID is made anonymous to unauthorized entities, but identifiable by the authorized entities.[4] As shown in Figure 2, IA-CAN uses a two-step authentication process: *anonymous ID (A-ID) filtering* (step one) to check the authenticity of the sender and *message authentication* (step two) to check the validity of data. The current A-ID is generated from the previously used A-ID (initially from original ID assigned to the frame type), and shared secrets are established by using a nonce per session. The shared secrets are composed of a pre-shared key and a shared secret from a previous transmission between authorized entities.

Today, each ECU uses a CAN controller to connect to CAN. The CAN controller applies a frame (message) filter that only allows CAN frames that have one of the selected CAN IDs to pass for further processing in the ECU. The overall idea is that IA-CAN randomizes the CAN ID by using cryptographic operations. This ID is used by a receiver to select messages from the CAN bus to read. During each time period, the sender needs to reset the ID that is in use to match what the receiver is expecting; otherwise, the sent messages will be filtered out. An attacker who does not know the new ID cannot even reach an ECU, and therefore cannot mount an attack (in the same way as you cannot rob a bank if you don't know the address).

In step one, IA-CAN uses the frame filter to check the anonymous ID of each received frame. Generating A-IDs on a per-frame basis enables the authentication of the sender. Only an authorized sender or receiver can generate or identify a valid A-ID using a shared secret key and a random nonce. The receiver ECUs update their filters by pre-computing the A-ID and, upon receiving a frame, filter it. The ID is altered or anonymized on a per-frame basis and invalid frames are filtered without requiring any additional run-time computation. Since each A-ID is used only once, the attacker does not gain anything from reusing the captured A-ID (i.e., replay attacks are not possible).

Step two is designed for the potential attack scenario that a physically compromised device modifies

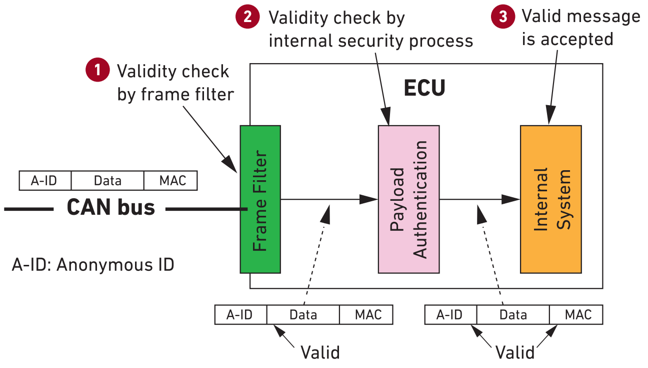


Figure 2 | Two step-authentication processes of IA-CAN.

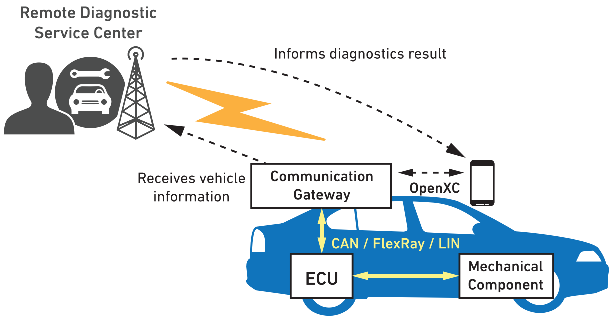

Remote Diagnostic Service Center
Informs diagnostics result
Receives vehicle information
Communication Gateway
OpenXC
CAN / FlexRay / LIN
ECU
Mechanical Component

Figure 3 | An example of a recent connected vehicle application: remote diagnostic service.

messages by violating the CAN arbitration rule (a mechanism to detect and mitigate that two CAN devices send at the same time on the bus). The payload data is verified by using a cryptographic message authentication code (MAC). This prevents the attackers from modifying frames by overriding bits on the CAN. If message modification in CAN is not expected (e.g., there is only a single CAN bus that physically does not allow message modification), step two can be omitted.

The generation of the next time period's A-ID is done in idle time (while waiting for the next frame), and there is no run-time delay. The run-time overhead for step two is incurred only after the frame filter accepts the frame. While payload data authentication incurs a small run-time delay, it is still the same as the overhead of previous CAN security models.

IA-CAN ensures resiliency against DoS attacks. Two types of DoS attacks are possible for CAN: a *flooding* attack that transmits a large number of frames to a target ECU, and a *starvation* attack that disturbs transmission over the CAN bus so that ECUs can't receive frames. If a flooding attack is mounted, the latency of IA-CAN is still constant and small while the latency of existing security protocols increases linearly to the point that the ECU is blocked. Against a starvation attack, ECUs can maintain listening frames after turning into a fail-safe mode, which is a major advantage for recovery planning.

Secure Connectivity Between Vehicles and External Devices

It's increasingly common for vehicles to establish communications between external devices (e.g., a central server) and the vehicle's internal ECUs through a communication gateway, as shown in Figure 3.

We've proposed a three-step authentication protocol that provides secure communication between the external device and the ECUs in the vehicle.[5] We consider the different nature of in-vehicle network and external networks in Table 1.

As depicted in Figure 4, the protocol consists of three phases: Phase 1 (**P1**) is the initial authentication of the

Table 1 | Comparison of different entities.

Device Type	Device Lifetime	Communication	Upgrade/ Replacement Frequency	Secret Information/ Key	Key Lifetime
User device	Short-term (months – two years)	• Wireless connection over 3G/LTE, Bluetooth • e.g., smartphone, tablet, etc.	Frequent over wireless access	Users can download over wireless communication	Short-term (hours or days)
Communication Gateway	Mid-term (years)	• Connected to the user device and the CAN bus only • e.g., built-in (i.e., part of telematics) or an OBD-II dongle (as in the case of OpenXC)	Rare over limited access (mostly physical access)	Key initialization during initial purchase with system update available after physical detachment	Mid-term
INTERNAL ECU	Long-term (equal to a car's lifetime)	• Connected to the CAN bus only • e.g., internal components in the car	Only replaced when broken	Built in by manufacturer	Long-term (equal to device's lifetime)

detachable communication gateway (e.g., OBD-II dongle) over CAN. Phase 2 (**P2**) is the mutual authentication between the external entity and the gateway ECU over Bluetooth (or USB). Phase 3 (**P3**) is the authentication of the external entity's data request.

The protocol is secure against all possible attack scenarios we analyzed previously in this article. Using a short-term key as in Table 1, the risk from key extraction is limited. The gateway is considered trustworthy once it is connected to the vehicle by P1 and the user's device stores only a short-term secret. Impersonating a user's device or a gateway is prevented by P2. P3 prevents fraudulent requests from a compromised user's device and fraudulent requests from a compromised gateway.

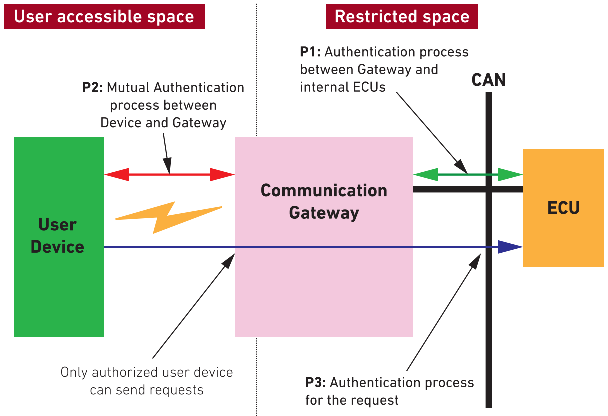

User accessible space
Restricted space
P1: Authentication process between Gateway and internal ECUs
CAN
P2: Mutual Authentication process between Device and Gateway
User Device
Communication Gateway
ECU
Only authorized user device can send requests
P3: Authentication process for the request

Figure 4 | Three-step authentication for secure connection between external entities (user device) and ECUs (CAN).

Conclusion

The importance of automotive cybersecurity is rapidly increasing. Although there have been efforts to implement secure solutions, many problems remain unsolved. We have introduced the IA-CAN protocol that provides strong protection against DoS attacks, and a three-step authentication protocol that provides secure integration of external devices with the vehicle's electronics. These solutions are practical automotive security approaches for in-vehicle architecture and advanced connected vehicle applications.

__Dr. Kyusuk Han__ is a Research Fellow at the University of Michigan, where his current research interest is automotive cybersecurity. He received his M.S. in Computer Engineering, Information, and Communications and his Ph.D. in Information and Communications Engineering at Korea Advanced Institute of Science and Technology (KAIST). During his Ph.D. course, Han studied security protocols for 3GPP mobile network and wireless sensor network.

__Dr. André Weimerskirch__ is an Associate Research Scientist at the University of Michigan Transportation Research Institute (UMTRI). Weimerskirch holds a Ph.D. from Ruhr-University Bochum, Germany, in the area of applied data security and a Master's in Computer Science from Worcester Polytechnic Institute. Before UMTRI, Weimerskirch co-founded the automotive cybersecurity company ESCRYPT that was sold to Bosch in 2012, and was in charge of ESCRYPT's American and Asian operations with offices in the U.S., Japan, and Korea.

__Dr. Kang G. Shin__ is the Kevin and Nancy O'Connor Professor of Computer Science and Founding Director of the Real-Time Computing Laboratory in the Department of Electrical Engineering and Computer Science at the University of Michigan. He received M.S. and Ph.D. degrees in Electrical Engineering from Cornell University. Shin's current research focuses on QoS-sensitive computing and networks as well as on embedded real-time and cyber-physical systems.

REFERENCES

[1] RiskIQ. "RiskIQ Reports Malicious Mobile Apps in Google Play Have Spiked Nearly 400 Percent." Feb. 19, 2014. Retrieved from http://www.riskiq.com/company/press-releases/riskiq-reports-malicious-mobile-apps-google-play-have-spiked-nearly-400.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In D. Wagner, ed. Proceedings of USENIX Security 2011. USENIX. Aug. 2011.

[3] Charlie Miller and Chris Valasek. "Adventures in Automotive Networks and Control Units." 2013.

[4] K. Han, S. D. Potluri, and K. G. Shin. "Practical Real-Time Frame Authentication for In-Vehicle Networks." escar USA 2014. June 18-19 in Ypsilanti, MI.

[5] K. Han, S. D. Potluri, and K. G. Shin. "On Authentication in a Connected Vehicle: Secure Integration of Mobile Devices with Vehicular Networks." Proceeding of ICCPS 2013, pp. 160–169. Apr. 2013.

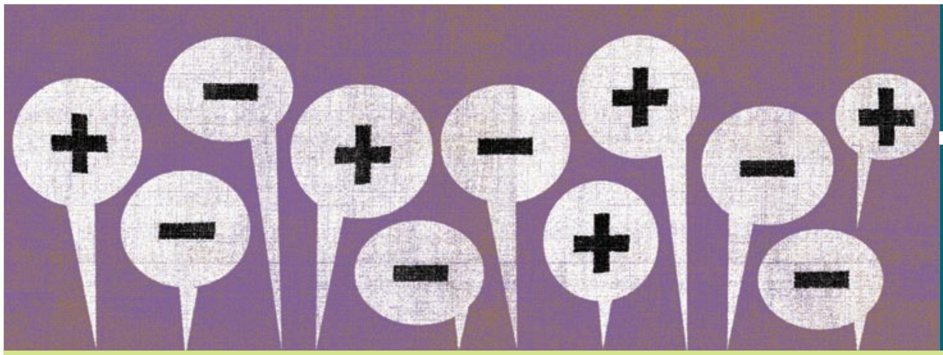
[6] D.K. Nilsson, U.E. Larson, and E Jonsson. 2008a. "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes." In Vehicular Technology Conference, 2008. VTC 2008-Fall, IEEE 68th. 1–5.

[7] Chris Szilagyi and Philip Koopman. 2010. "Low Cost Multicast Authentication via Validity Voting in Time-Triggered Embedded Control Networks." In Proceedings of the 5th Workshop on Embedded Systems Security. 10. http://dx.doi.org/10.1145/1873548.1873558.

[8] Hendrik Schweppe, Yves Roudier, Benjamin Weyl, Ludovic Apvrille, and Dirk Scheuermann. 2011. "Car2X Communication: Securing the Last Meter." WIVEC 2011, 4th IEEE International Symposium on Wireless Vehicular Communications, 5-6 September 2011, San Francisco, CA, United States (June 2011), 1–5.

[9] Bogdan Groza, Stefan Murvay, Anthony van Herrewege, and Ingrid Verbauwhede. 2012. "LiBrA-CAN: a Lightweight Broadcast Authentication Protocol for Controller Area Networks." Proceedings of 11th International Conference, CANS 2012, Darmstadt, Germany. (December 2012), 185–200.

[10] Oliver Hartkopp, Cornel Reuber, and Roland Schilling. 2012. "MaCAN - Message Authenticated CAN." escar 2012, Embedded Security in Cars Conference 2012, Berlin - Germany (November 2012).



TECH
CORNER

To supplement the ***IQT Quarterly***'s focus on technology trends, *Tech Corner* provides a practitioner's point of view of a current challenge in the field and insight into an effective response.

TELEMATICS AND WEATHER DATA SCIENCE CONVERGE

A technology overview from IQT portfolio company Weather Analytics

The state of the atmosphere's impact on vehicular travel looms large.

Weather conditions cause or exacerbate an estimated one-fourth of all roadside accidents. The need for local, current, and relevant weather information is paramount to understanding and improving vehicle operations across consumer and commercial markets. With the rise of connected vehicles, meeting this need becomes possible. Using live feeds of weather data to send alert notifications is a major — and intuitive — safety precaution.

However, optimizing safe travel requires up-to-date weather information on a highly localized basis, and current weather broadcast companies aren't designed to go along for the ride. Continually refreshing The Weather Channel app on your phone while driving is unwieldy (and should get you pulled over!).

Additionally, the advent of telematics poses other questions and challenges to be addressed by vehicle manufacturers, regulators, insurers, and weather information companies. For example, new initiatives such as route-optimization analysis and usage-based insurance (UBI) programs spawn the need for both situational awareness and contextual and historical data. Using historic weather data better informs the whole picture of connected travel.

One solution is integrating a connected vehicle into regularly-refreshed, current, and forecast conditions that are geotagged with the movement of a vehicle. Such integration goes a long way toward improving travel safety and trip optimization. The best way to optimize frequently isn't readily apparent, though. Sending real-time weather information to (and from) fleets of traveling vehicles is important, but still relies on the drivers' or managers' intuitive and immediate sense of how to respond to the information.

This juncture is where telematics technologies and weather data science converge. Recent advancements in large-scale computational modeling allow hyper-local weather reporting — an important part of the telematics solution. Weather Analytics is a global leader in using such models. It has leveraged them to create a high-resolution, globally gap-free weather database capable of solving problems arising from a widespread, multi-nodal network of vehicle connectivity.

Back to the Future

Making the most of connectivity requires a robust calculation that ties together vehicle speed and direction, outside conditions, types of cargo, and so forth. Historic information — inside and outside the vehicle — is needed to map losses and efficiencies.

When 7PSolutions, a global logistics and fleet management outfit, tracks hundreds of its connected vehicles carrying temperature sensitive pharmaceuticals, it can only make so many decisions about which routes will likely prevent the most accidents based on its organic data alone. By converging past spoilage reports with local, hour-by-hour historic

temperature, precipitation, and humidity data, hyperlocal reporting by Weather Analytics offers a layer of optimization not previously available. For example, if rates of spoilage peak when vehicles travel through four hours of sustained temperatures of 90 degrees compared to a brief 30-minute break into cooler (70 degree) temperatures, this calculation can offer an impactful insight in how to best re-route particular vehicles in the "cold chain."

When you add to this data analysis information about speeding, accidents, terrain, and a host of other relevant variables, then a more complex web of optimization becomes apparent. Even in instances where no vehicle or route data previously existed, using 34 years of historic weather data can establish baseline optimization profiles for key travel routes on a highly granular basis. Such business intelligence can especially benefit small and medium-sized companies facing high barriers to entry in the competitive logistics market.

Future Data: Technological Collaboration

This process of data collection and convergence is ongoing. Even as the real-time alerting of weather conditions is valuable to the driver or fleet manager for tactical adjustments, every trip is also collecting (and creating) data that is valuable to larger strategic challenges. Before the advent of live telematics, travel-related data collected (for example, spoilage reports) was rudimentary, retrospect, and heuristic.

Yet telematics companies are now ingesting a complex web of data that lends itself to precise and robust data science. One leading insurance company in the telematics space has already logged data reports covering more than 5 billion miles of travel. At the same time, there is a need for an on-the-ground context — clean and rationalized enough to make access easy — to make sense of all of this data.

With the onslaught of data, we are able to solve challenges that are emerging with the advent of recent technologies. The rise of the electric vehicle (EV) raises several questions about fuel and financial efficiency. The reliance on batteries may reduce our dependence on traditional fuels, but there still exists an ideal set of conditions for efficient use — most of which revolve around temperature.

Unlike gas-powered cars, EVs can see increased life and usage by optimizing the life of the battery through temperature control. Ingesting weather data into the simulations and models of EV battery testing can improve the efficiency and production of batteries. While we can't change the weather that occurs outside, nor can we always change the route the driver takes (especially in consumer markets), knowing the thermal context in which particular EVs are likely to exist can inform the manufacturing of the batteries — as well as the trade-offs in car manufacturing.

Other questions also arise: Is it worth adding weight or space to a vehicle body for a more insulated battery — or is the car only going to drive in cool or mild climates? Weather data allows us to step away from a one-size-fits-all model of production and tailor cost-effective and context-effective strategies.

Telematics also tells us a lot about traffic congestion. Prior to connectivity, traffic patterns were based predominantly on visual (helicopter) and tactile (vehicle tracking pads) data points. Now, having a web of sensors inside several cars during a buildup provides new insight at a much faster pace. Being able to fuse this

Telematics companies are now ingesting a complex web of data that lends itself to precise and robust data science.

time-coded and geo-stamped traffic data with hyper-local weather data will help inform policy, infrastructure planning, and consumer travel plans.

Problematic Telematics

Yet as consumers are increasingly expected to be the drivers (pun intended) of telematic adoption, fears abound regarding whether these connectivity tools are of the benefit to the consumer — or solely aid those looking to control and monitor driving behavior. UBI is one such program that seeks to glean information from drivers in order to write insurance policies (and set premiums) based on activity.

As John Lucker of the consulting firm Deloitte states in a recent study on UBI, "Insurers can watch you drive." The push for connected vehicles holds great promise for insurance companies. Benefits can include better understanding the risks they are being asked to underwrite when they extend coverage — and more knowledgably price their policies. At the same time, the Deloitte study indicates that 47 percent of consumers report not wanting their vehicle tracked, regardless of any discounts they may stand to gain on their policy. It appears there needs to be an even greater value-add experience for customers to feel comfortable with UBI. Weather information may be the answer.

By plugging in weather conditions, consumers are given important, on-demand weather information related to their journey that doesn't compromise their privacy. Safety alerts and driving tips can add to the "gamification layer" that companies like Deloitte are trying to push for UBI products. Forecast inputs can play a large role in convincing drivers of the value of driving "connected."

Telematics is live, two-way communication. It poses several challenges — especially in the consumer market — but also many opportunities to learn from and improve our vehicular ecosystem. At the heart of the mission, telematics is a way of collecting and distributing live feeds of data. Understanding the world outside the vehicle — the state of the atmosphere — is critical to harnessing the value of telematic communication. Q

***Weather Analytics**, an IQT portfolio company, delivers global climate intelligence by providing statistically stable, gap-free data formed by an extensive collection of historical, current, and forecasted weather content, coupled with proprietary analytics and methodologies. To learn more, visit www.weatheranalytics.com.*

FROM THE PORTFOLIO

The *IQT Quarterly* examines trends and advances in technology. IQT has made a number of investments in innovative technologies, and several companies in the IQT portfolio are garnering attention for their unique solutions.

GainSpan

GainSpan is a fabless semiconductor company focused on connecting devices wirelessly to the Internet. The company recently announced a full HD-resolution video application development kit (ADK) targeting Internet of Things applications in the automotive, surveillance, and security markets. The ADK is a complete hardware and software platform that accelerates time to market for customers seeking to add high-quality IP video streaming to their products. GainSpan is based in San Jose, CA, and has been an IQT portfolio company since March 2009. **www.gainspan.com**

Looxcie

Looxcie manufactures a wearable camera system for mobile, hands-free video capture and sharing. The company's Vidcie head-mounted camera was referenced in a *Wired* article on the future of wearable applications in the workplace, where field technicians can send live video of a problem to colleagues and collaboratively troubleshoot it. Looxcie joined the IQT portfolio in October 2011 and is located in Sunnyvale, CA. **www.looxcie.com**

Mocana

Mocana provides a device-independent security platform that secures all aspects of mobile and smart connected devices, as well as the apps and services that run on them. The company was recently mentioned in several online publications including *InformationWeek* and *SecurityWeek* for its response to the Heartbleed vulnerability. Mocana's security experts called the revelations a "wake-up call," and urged developers of smart connected devices to ensure their products are secure, private, and safe. The company is based in San Francisco, CA, and has been a part of the IQT portfolio since March 2012. **www.mocana.com**

Signal Innovations Group

Signal Innovations Group (SIG) provides signal, image, and video analytics for government and commercial applications. The company's Tracking Analytics Software Suite (TASS) provides accurate, real-time detection and tracking of thousands of vehicles through challenging lighting conditions, dense traffic regions, and kinematic dynamics. SIG Scout is a compact hardware solution that uses TASS for airborne tracking of moving targets in full motion video imagery. The company is located in Durham, NC and became an IQT portfolio company in March 2010. **www.siginnovations.com**

IQT®

IN·Q·TEL