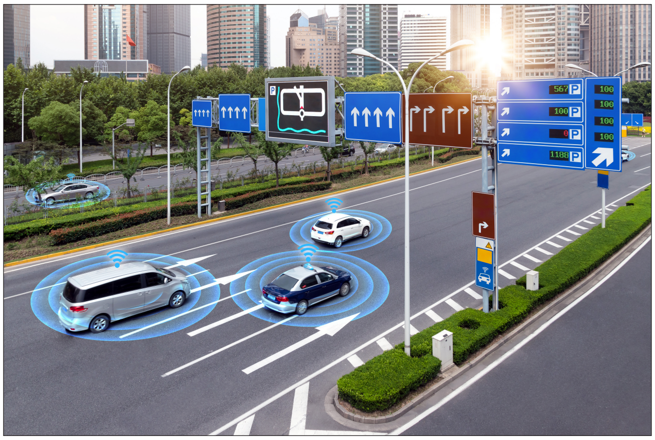
The Internet of Vehicles (IoV) — Security, Privacy, Trust, and Reputation Management for Connected Vehicles

Adam Drobot, OpenTechWorks Inc. and Tao Zhang, NIST,
with Mary Lynn Buonarosa, Frank Kargl, Steve Schwinke, and Biplab Sikdar

The IEEE IoT Magazine hosted a Virtual Roundtable to discuss the technologies, business models, governance regimes, and public perceptions of the challenges and opportunities for solutions to issues of security, privacy, and trust for connected vehicles.

In conducting the Virtual Roundtable, we developed a list of fifteen questions that spanned the range of touchpoints where connected vehicles relate to the Internet of Things and specifically the issues surrounding security, privacy, and trust. We sought to capture viewpoints that are important to automotive OEMs, their suppliers, technology providers, the consumer, regulators, and finally to overall public perception. In that context, to achieve public acceptance for the evolving mix of connected vehicles we also addressed the subject of reputation management. The Virtual Panel consisted of four experts who include: **Mary Lynn Buonarosa** from the University of Michigan Transportation Research Institute, **Frank Kargl** from the Institute for Distributed Systems at the University of Ulm, **Steve Schwinke**, from Sibros Inc., a developer and supplier of platforms for managing software and applications for connected cars, and finally **Biplab Sikdar** from the National University of Singapore who has served as Editor of IEEE publications on Mobile Computing, Vehicle Technology, and IoT.

We first shared the questions with our four experts and then had them join us in a virtual online session. We asked them to respond to each of the questions without preparation and to provide answers only to the questions that they were comfortable with. The session lasted two hours and was recorded. We manage to go through ten of the fifteen prepared questions during the session, and these are the subject of the discussion for the virtual panel. The recording was transcribed and lightly edited. Each of the experts was then given a chance to provide a final edit of their responses. The material that follows is based on the opinions of our experts, as much as possible in their own words. We hope that the questions and answers will shed light on the important challenges and opportunities for connected vehicles and provide insight for developing beneficial and safer solutions.



Roundtable Moderators

Adam Drobot is the Chairman of the Board of OpenTechWorks, Inc. His activities are strategic consulting, start-ups, non-profits, and industry associations. In the past he was the President of Applied Research at Telcordia Technologies (Bellcore) and the company's CTO, and before that the Senior Vice President for Science and Technology at Saic/Leidos. He is a current member of the FCC Technological Advisory Council where he Co-Chairs the Working Group on Artificial Intelligence. In the past, he was on the Boards of the Telecommunications Industry Association (TIA) where he Chaired the Technology Committee; the Association for Telecommunications Industry Solutions (ATIS); the US DoT ITS Program Advisory Committee, and the University of Michigan Transportation Research Institute External Advisory Board. Over the years he has been active in IEEE including the IEEE IoT Activities Board, and multiple major conferences such as the IEEE World Forum on IoT. He is currently a member of the IEEE Press Editorial Board. His degrees include a BA in Engineering Physics from Cornell University and a Ph.D. in Plasma Physics from the University of Texas.

Tao Zhang, an IEEE Fellow, has been leading research, product development, and corporate strategies. He is currently managing the Transformational Networks and Services Group in the Communications Technology Lab at the National Institute of Standards and Technology (NIST). He was the CTO/Chief Scientist for the Smart Connected Vehicles business at Cisco Systems, and the Chief Scientist and a R&D Director on wireless and vehicular networking at Telcordia Technologies (formerly Bellcore). He cofounded the OpenFog Consortium and served as a founding Board Director to spearhead global fog and edge computing efforts in the industry and academia. Tao holds ~60 US patents and coauthored two books "Vehicle Safety Communications: Protocols, Security, and Privacy" and "IP-Based Next Generation Wireless Networks." He served as the CIO and a Board Governor of the IEEE Communications Society and as a Distinguished Lecturer of the IEEE Vehicular Technology Society. He cofounded and served on leadership roles for multiple international conferences and forums.

Roundtable Panelists

Mary Lynn Buonarosa is a project manager in the Human Factors Division at the University of Michigan Transportation Research Institute. Currently, she serves as the program manager for the Smart Intersections project which is developing an infrastructure-assisted cooperative driving automation testbed to accelerate connected and automated vehicle deployment. Previously, she was the deputy program manager for the Ann Arbor Connected Environment, the world's first combined connected vehicle and infrastructure deployment. She has more than 25 years of automotive research experience including planning and executing program plans; stakeholder management; experimental design; and data analyses of large naturalistic, driving data sets. Her research interests focus on vehicle-to-vehicle and vehicle-to-infrastructure deployment and safety applications; advanced driver-assistance systems; vulnerable road user safety; and teen driving.

Frank Kargl is a Professor at the University of Ulm and Director of the Institute for Distributed Systems. He received his doctorate in 2003 and his habilitation in 2009 at the University of Ulm. Before that he was, among other things, a co-founder of the Argo Inc., and responsible for network operation and security in the network group of the data center/KIZ of the University of Ulm. Between late 2009 and early 2012 he was an Associate Professor in the Distributed and Embedded Security (DIES) group at the University of Twente in the Netherlands, then adjunct professor until January 2016. Since February 2012, Prof. Kargl has headed the Institute for Distributed Systems at the University of Ulm. From October 2013 to September 2016, he served as Vice Dean of the Faculty of Engineering, Computer Science and Psychology, of which he was then Dean until September 2018. Prof. Kargl is a member of the ACM, the IEEE, the Society for Computer Science, Gesellschaft für Informatik and the specialist groups for security and KuVS (Kommunikation und Verteilte Systeme).

Steve Schwinke is Vice President of Customer Engagement at Sibros Inc., working closely with OEMs and Tier One suppliers to accelerate their connected vehicle solutions. He is a pioneer in the industry having spent 22 years at General Motors as an original Executive member of the OnStar team designing their first 3-button system, developing, and launching numerous industries first connected vehicle products and services. He is a recognized expert in connected vehicle technology having served on the Executive Board of Directors for the Telecommunications Industry Association and has been awarded 34 patents involving telecommunications, telematics, and navigation. Steve holds a Bachelor of Science in Electrical Engineering from the University of Michigan and a Master of Science in Wireless Communication Systems from Santa Clara University.

Biplab Sikdar is an Associate Professor in the Department of Electrical and Computer Engineering at the National University of Singapore (NUS), where he also the acting Head of Department for the Department of Electrical and Computer Engineering. At NUS, he also directs the US$40 million corporate research lab with Cisco Systems. He received the B. Tech. degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, in 1996, the M.Tech. degree in electrical engineering from the Indian Institute of Technology, Kanpur, India, in 1998, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He is a recipient of the NSF CAREER award, the Tan Chin Tuan fellowship from NTU Singapore, the Japan Society for Promotion of Science fellowship, and the Leiv Eiriksson fellowship from the Research Council of Norway. He is a distinguished lecturer of IEEE and ACM and has served/serves as an Associate Editor for the *IEEE Transactions on Communications*, *IEEE Transactions on Mobile Computing*, *IEEE Open Journal of Vehicular Technology*, and *IEEE Internet of Things Journal*.

IEEE IoT Magazine: Let us start off with the first question for the panel. We live in a world of rapid technological advancements. Vehicles are becoming increasingly sofwareized and connected, which is changing how they are designed and used. What do you see driving the changes in technology for connected vehicles and how do you see the changes impacting connected vehicle architecture, supporting infrastructure, and ecosystem? What do you see as the most important things that are going on at the intersection of public perception and the technology that's going into vehicles?

Steve Schwinke: I think there are two major shifts going on. From the consumer standpoint, users see connectivity and they see the adoption of electrical vehicle (EV) technologies. So, what you have, especially around EVs, are exciting new entrants in the marketplace. OEMs (Original Equipment Manufacturers) traditionally have had a large barrier to entry for new competitors in the resources necessary to develop ICEs (Internal Combustion Engines). With the simplification that comes with EV technology, you see new entrants coming into the marketplace, but at the same time they are also far behind in their learning curve. In contrast you've 120 years of experience in building and supporting ICEs. So that's where connectivity really comes into play — as you put these new vehicles into the market, how do you get that rapid feedback from a connected mobility product to understand how that product is performing, how it's being used, and how you can update it, so you don't have to go through the long cycles that we had with ICEs. Traditionally, the customer takes delivery of the vehicle, they find problems, they go back to the dealership, the dealership finds out what went wrong, tries to diagnose it, then send the issues back to the quality departments at the OEMs. This is a very long cycle. So, with EVs, we see that the new entrants who really embrace connectivity are going to be the winners, because they're going to be able to quickly fix problems and make changes to the vehicle to make sure that it's delivering what the customer experience needs to be. There's also a whole multitude of changes going on with electrical vehicle architectures.

Biplab Sikdar: Yeah, I think one of the interesting things is electric versus connected. For example, in our university's campus, which is about a mile wide, we have shuttle buses running over multiple routes. All the buses are electric but are not really connected yet. So, what I am thinking is whether we understand completely how to fully exploit the benefits these vehicles can bring. We do need to be connected, but in the short term we have to consider the tradeoffs between privacy and security issues that connectivity creates, and the total benefit in terms of optimization, efficiency, and environmental impact that comes along with connectivity.

Frank Kargl: I see timing as an important factor in the development of new cars. When I entered the automotive domain in 2005, electronics had already been introduced as an important element in cars, then connectivity became an additional factor. From a security and privacy perspective, this created a problem as cars became accessible not only to OEMs but also to almost anyone, including malicious actors. Basically, this set the stage for the need to actively defend cars. It also created the realization that when the cars could continuously produce data, they could also affect privacy. This was also the time, when here in Europe, General Data Protection Regulations (GDPR) was established. There was always this tension between additional data introduced by connected vehicles and the weak laws to protect the privacy of the people traveling in their vehicles. Since then, my focus has been expanded, I would say by two additional factors. First is autonomous driving, which puts a lot more responsibility on the vehicle and changes the privacy and security models. The second aspect is that we are now talking a lot more about cooperative and autonomous mobility that is enabled by connectivity. These cooperative systems would, for example, coordinate when they enter an intersection, which brings yet another level of complexity to the overall systems. I think that this is also a challenge for security because these systems are complex and need to be managed and maintained; otherwise, we will not be able to comprehend and evaluate full system functions. This will mean they will not be trustworthy anymore. I think it's the same factors that we see for connectivity, autonomy, and for cooperative behaviors.

Mary Lynn Buonarosa: I think safety will continue to be a big driver for customers. While we have seen fatality rates coming down over time, in the last several years, during the pandemic, we saw a sharp increase in fatalities, in spite of the fact that most of us were working from home for more than a year. Alarmingly, vulnerable road user fatalities are increasing. Over 42,000 people were killed on US roadways in 2021. I think that connectivity will increase safety. When I'm speaking about connectivity, my experience is around connection of vehicles to each other and to the surrounding infrastructure, sending and receiving messages for safety applications. The Intelligent Transportation Systems (ITS) band, 5.9 GHz, is what we originally used for communications in Ann Arbor. We deployed Dedicated Short-Range Communication (DSRC) devices. With the FCC (Federal Communications Commission) Report and Order in late 2020, we no longer broadcast using DSRC, as 60% of the frequency band has now gone to unlicensed users. Consequently, we're using the upper30 MHz, and use - cellular vehicle-everything (C-V2X) devices. Largely that will be for safety messages to vehicles, between vehicles (V2V), and between vehicles and the infrastructure (V2I).

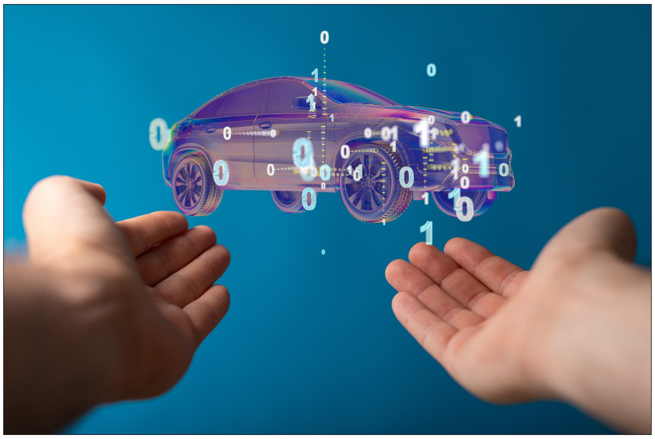
IEEE IoT Magazine: The next question has to do with the forces driving the push for privacy and trust. As you know, there are many things that drive privacy and trust requirements. What do you see as the main forces for privacy and trust for connected vehicles and how do the solutions that are deployed affect important requirements such as availability, reliability, driver perception, and overall security?

Frank Kargl: Let's talk about trust and trustworthiness of these systems first. In these European projects that I mentioned (https://www.sevecom.eu/, https://horizon-connect.eu/) we are basically following a technical notion of trust. We want to develop trust models that would allow us to formally reason about effects. For example, if a part of the system gets compromised, say one Electronic Control Unit (ECU) in a vehicle gets hacked, what would be the effect on the trustworthiness of typical automated functions? These functions may be in some totally different parts of the system. We want to have these technical trust models to quantify and reason about trust. We also have people from the University of Twente, who have a sociology and psychology background. Another question we have is, how can this technical notion of trust be brought together with the user-perceived trust? The idea is that if we cannot technically assess how trustworthy a system is, then it's hard to trust the system. You need some evidence for trust. For example, if your vehicle is operating on trustworthy data and you can identify that it is making good and reliable decisions, that serves as evidence. Only if this is in place, can you then provide evidence to the passengers, so that they can trust the system. And the more complex the system gets, the harder it will be to communicate this if you don't have a good underlying model and idea of the trust relationships in your system.

Steve Schwinke: When I think about trust, it implies that you must have transparency with your customers and make sure you have their consent. Transparency is being very clear with what data you're collecting and for what purposes, giving your customer the choice to decide whether and how that information will be used or shared, and the ability to stop data collection and delete the data that has been collected. Keeping it very simple and very transparent for customers is how you build trust. If someone has a security breach, like we just recently saw with a satellite service provider of audio systems, it creates a black eye and a problem for the entire industry. It raises awareness, but also makes everyone nervous. So, this is an industry problem, and we all must operate with the highest levels of integrity around transparency, consent, and the right to choose. I talked a little bit earlier that it's the OEMs responsibility for providing transparency to customers, and we give them the tools to implement solutions. At the same time, you also must consider what the OEM needs, which completes the feedback loop. There's a lot of goodness around getting data from the vehicle. I'm happy to explore that a little bit more with Mary Lynn — the importance of understanding vehicle safety and how to help OEMs improve their products. But it's another thing when you want to take the customer's data and provide it to a third party, that should always require explicit customer consent. You have to be trustworthy, then you have to make sure that every time you're going to use that data for marketing, that you're very explicit about what information you're going to share and get customer's consent before you do it. So, as an industry, we all have to very diligent about what we do with the data. You can't have even one bad actor out there because it will tarnish the entire industry.

Mary Lynn Buonarosa: I agree a lot. I think people should have to opt in as opposed to opt out in order to have their data sold to third parties. I think that is really important and the consent choices shouldn't be buried on page 56 of lengthy agreements. It should be stated, really upfront, that some of these data will be used to inform safety or increase mobility, and allow the consumer to reap the benefits, but then not have the data sold to third parties unless customers want it to happen. It is important to allow people autonomy over what happens to their data. Then finally, what we've heard from a lot of people that are participating in our studies, is the question: "Will I be tracked?," and people really want to know. Most of us all begin our days at home, so with the GPS coordinate data for the beginning of our first trip, trips in between, and the last point is each trip, it is possible to find the way to our kids' schools, where we pursue entertainment, and these kinds of things. People want to know that they're driving anonymously, and that they can't be tracked. That is an important concern.

Biplab Sikdar: Yeah, I agree completely with what Mary Lynn, Steve, and Frank said earlier. The other part of the whole equation is how some of the privacy preserving technologies that we were putting into place may affect the utility of our connected vehicles. For example, if I want to preserve my location privacy, I can add noise to what my current location is. But then that can affect, for example, safety applications or other location-based services that I might be interested in. So again, there might be a tradeoff between how much privacy I want versus the utility or value I can expect of the system. This may have to be explored in more detail as we go along.



IEEE IoT Magazine: So, let's go on to the next question, which we may have covered a little bit already. How can privacy and trust requirements in IoV be fulfilled — for both OEMs and vehicle operators? How are the forces that drive the requirements evolving? How do you see them change in the near and far future? We have all mentioned autonomous vehicles. Looking at SAE's (Society of Automotive Engineers) five levels of driving autonomy, we still have a little way to go. So, that is the far future, but the use of connectivity is in place already. There are additional things like the use of AR (Augmented Reality) and VR (Virtual Reality). We already see almost every OEM having the systems that, for example, read speed signs, and things of that sort. Again, those systems must be trusted. On the legislative front, there are laws like GDPR in Europe, and US states like of California and several others have also enacted legislation. Lastly, the extensive use of AI that can bring in a lot of phenomena that we never expected.

Steve Schwinke: I think there's a long road to get to Level-5 automated driving. We're just touching the surface of Level 4. Most automotive offerings are mainly for Level 2. These systems try to make our roadways safer for everybody. I know that University of Michigan Transportation Research Institute (UMTRI) is very involved with safety. We heard from Mary Lynn that fatalities are going up. I don't know all the causes of that, but I do know that it's a problem. I can't imagine anyone on this panel who hasn't been affected and touched by roadway safety. So, I think we should look at new advanced features such as crash imminent braking, lane keeping assist, and study how good they are. How effective are they? How many false positive and false negative events are occurring? Can we improve these systems so that we can make them more effective and our roadways safer? Also, you can't manage something if you can't measure something. So, let's always start with the goodness of why we collect and have connected vehicle data; it's to make our systems better and our roadway safer. That's where I always start the conversation in terms of understanding our product performance, what can we do to improve safety, which is important. I get passionate around this also because it dovetails into other things. So, you think about a safe driver app that GM puts out, which is really interesting. It could involve more data elements from the vehicle to help teen drivers and everyone else be a safer, better driver. Who can argue about that, but then you dovetail that into, well, I'm going to sell that data to insurance companies. That's okay as long as it has explicit customer consent before you sell that data. So, let's start with why it's so important to have that information. But then when we do expose it to third parties, let's make sure we get explicit customer consent before that's done. If you follow these guidelines, I think you're always going to be on the safe side of what we're trying to do as an industry, which is to try and ultimately create a better experience and also make our roadways safer for everybody.

Biplab Sikdar: I agree that, in this context especially in Asia, governments have a big role to play. Ultimately, it's the rules and laws that will get all actors to fully comply or at least put in mandated measures to ensure that the privacy of all parties involved are respected and taken into consideration.

Frank Kargl: Consider automated driving, we see that the push for higher automation levels is fully on. When you look at what Tesla's currently trying — Full Self-Driving (FSD) — that's a good example. In Europe, here, things are moving a little bit slower, because I think regulations are more complex. But nevertheless, I think there will be a development here in Europe too. This will inevitably mean that more data is collected and processed. We will have substantial amount of AI (Artificial Intelligence) mechanisms involved. The privacy implications of machine learning systems are still not 100% clear in our research. We study privacy preserving machine learning, but in the end, I think connected and automated driving will be a trend and a development that cannot be stopped. So, from the privacy perspective, the question is, how do we deal with it? I mean, we have been introducing privacy enhancing technologies. For example, in V2X communications, we had changing/dynamic pseudonyms that should help alleviate at least a small bit of privacy concerns arising from trip data with the start and stop pairs that Mary Lynn mentioned. I think this is important to not lose sight of privacy, not only when it comes to consent and transparency, which are all important elements, but also other privacy aspects covered by, for example, GDPR. This includes a lot about technical and organizational measures that need to be put in place. So, we need to actively introduce the appropriate technology. Sometimes you call it privacy by design — technological mechanisms that inherently make the systems more privacy friendly.

IEEE IoT Magazine: You know, you mentioned GDPR, but the EU recently introduced something called the AI Act, which includes, besides AI, almost all forms of software. In some way, that takes the action away from, the experts, which would be the OEMs. One could say that this creates, for lack of a better word, a new bureaucracy that has the job of risk assessment of that software that may be on vehicles and so on. It looks like the legal regime seems to have moved faster than the lessons learned from actual practice,

Frank Kargl: That was a problem with GDPR from the start. Here in Europe, we introduced GDPR. It basically requires technical and organizational measures, and then everyone ends up discussing and debating what they really are. But it's basically an open question, what is the state of the art in privacy enhancing technologies that you would expect industry to adopt? There has been a lot of debate. For example, in cryptography, such as attribute-based credentials, and whether these technologies are something that industry would have to take into consideration. But there was never a catalogue where experts can agree on the state of the art. These techniques may be bleeding edge research that you could not expect industry to adopt. I think it's similar now with AI, not only for privacy but also for other risks related to AI. I think we are missing a clear understanding — what are acceptable risks and what are risks that require additional mitigations? When you look at adversarial examples, such as model inversion attacks, that could put the privacy of people who provide data for training at risk. So, I fully agree, we have a new space with a lot of new risks, and at the same time, legislation now wants to define what is acceptable and what is not. We are at a point where maybe even the experts don't fully understand these risks. So, I'm with you that going too fast with legislation is a waste. But of course, at the same time, not doing any legislation and leaving it fully to the industry might also not be the path to take.

Steve Schwinke: Frank, these aspects are really interesting, and I hadn't thought about them. But as you can tell, I get pretty passionate around roadway safety. I always envisioned a V2X communication technology when you're talking about 5G and a world in which pedestrians are broadcasting. The hardest part about automated vehicles is perception — understanding what that object is and what it's going to do next. I always envision a world in which anything that we care about is broadcasting information, as opposed to the vehicle trying to figure out what it is — is that a person riding a bike with a dog on a leash? That should somehow be broadcast to vehicles. We need cooperative behaviors. But then you talk about the privacy aspect of that broadcast signal which I find very interesting. That's at least how I'm interpreting your feedback, which I had never considered before. Because I always think, well, there's only good that can come out of me telling this automated vehicle that I'm here on my bike with my dog, please don't hit me as opposed to the vehicle trying to figure it out on its own.

Biplab Sikdar: I heard good points from everybody. I also agree that we cannot leave things to just the companies and expect them to do the right thing. Some amount of legislation is definitely necessary and has to go hand in hand with the technology that's being developed by the industry.

IEEE IoT Magazine: The next question is somewhat related. Are connected vehicle applications leading to new vehicle use patterns, new privacy, and security requirements, as well as new legislative and regulatory needs?

Mary Lynn Buonarosa: I think the short answer is yes, it will lead to all of those things downstream as people become more willing to make use of connected vehicle technologies and trust the ecosystem. What we're deploying in Ann Arbor, for example, are cooperative perception systems: here's a vehicle at the intersection, and a pedestrian may be blocked by another vehicle in that same intersection. There might be a partial system failure, or a sensor failure. Vehicles and the intersection can certainly provide information that there is someone on a bike or a pedestrian with a dog and they are moving together. We're using camera-based systems and driver-based systems in a collaborative driving system. We're just now beginning to deploy it this year. I don't have any data to report out now. But yes, and I think that as these are rolled out across states, and vehicles begin to trust the information they're receiving from other vehicles, and from the infrastructure, it will increase safety and mobility at intersections.

Biplab Sikdar: Yeah. I'm quite sure that connected vehicles will bring in new challenges in terms of privacy, security, and legislative requirements. In terms of how they would change our behavior in terms of new usage patterns and new applications. That's one thing maybe I'm not imaginative enough to think of those new things. But as far as the security aspects and the legislative aspects, definitely, there'll be some challenges.

IEEE IoT Magazine: To be more specific, let's say we look at navigation applications such as Waymo, that tries to optimize for the fastest way somebody can get somewhere. One of the consequences is vehicles spilling onto secondary or tertiary roadways. Conceptually that might violate the privacy of neighborhoods that don't expect such traffic. Are there patterns like that so that one really must watch out for annoying outcomes and avoid blowback against the technology?

Steve Schwinke: I see that drivers from the latest generation are more and more technical savvy, and they have more and more trust in how they use technology today. The most important thing is that you show value with trust. Do they see the value that comes from providing information about themselves, or about their vehicles, and then the value of connectivity itself. It's about customer experience as well as the benefits. On the customer experience side, they are going to see value, for example, when they don't have to go to a dealership for service of their vehicle and can get their cars fixed overnight while they are sleeping, as opposed to scheduling a three hour visit to a dealership to get a software upgrade. They are going to see the kind of value that they see today with their iPhones or their Android phones: these devices get updated automatically and customers would never expect to have to go back to the Apple store to get a software update. Why should the same thing not be occurring with our cars? If drivers see value, they're going to be more inclined to provide access to the data. If they can have a worry-free vehicle and will be more satisfied when maintenance is required, someone comes out to their vehicle and takes care of it for them. Time is the most important thing. Or if they can see the value of "fuel as a service" type of offerings, and more really good customer benefits from other services, you're going to see more trust around the usage of that data. If they see more and more just Marketing, Marketing, and Marketing pitches, then, there's going to be a problem. Today, I think, we're seeing people becoming more trusting about sharing their data because they're used to those pop ups on their phones, when the data will be shared, and an indication of the purpose. If they can see a tangible benefit, they're going to say yes, a lot.

Frank Kargl: I think I would like to introduce and focus on the word "purpose." Purpose binding and informed consent are important. I see from what we have been discussing, there are two very different types of connectivity or applications for a connected vehicle. We have been discussing about safety, critical applications, intersections, collision warnings, these are inevitable for road users. If we look at these types of applications, probably everyone would subscribe to them voluntarily to increase safety. But this is a type of local communication and a type of ephemeral data use. I think in this class of communication, we can all play. What the regulator could do, for example, is make sure that the data is not communicated long range, not persistent, and not stored, but is used in a limited scenario only. Then there are other classes of applications like ride hailing services and maintenance services where the intent is to centrally collect data, store it on a longer-term basis, and provide services to specific customers. This is probably a totally different type of data use and characterized by different types of data problems. This is what we have published in the past, for example, about solutions for anonymous privacy, preserving ride-hailing services. So, different technologies can probably help make systems that provide these services and at the same time, protect privacy to the maximum possible extent. It's not like, and I always want to avoid this impression, an either-or decision. It's not about either having the services and giving away privacy, or consenting to everything, or not using the services. I think privacy-enhancing technologies have come a long way to allow us to build systems that provide the right protection and useful and convenient services at the same time.

IEEE IoT Magazine: So, Frank, let us ask a question maybe sort of challenging an assumption. When we look at safety, one of the technologies in the OEMs toolchest today is the application of AI. That depends on safety data and therefore there is a premium on not making it ephemeral, but in fact making it available. It may be the case that we take what may be near-miss data and use the learnings from that to then avoid dangerous situations. Another example may be the use of black boxes or things of that sort on cars, the more importance is to understand and learn from primary safety data. It is important to share the data and learn from it collectively. This means storing it and processing it somewhere. Now, are we wrong on that? Or is that very much a trend at this point?

Frank Kargl: No, no, I mean, this is another type or class of safety applications. When you want to train machine learning systems on image data, you want to store this data for later training and for homologation (granting of approval by an official authority). So there, we indeed have another challenge. You could of course, put blackout blurs over visible license plates or the faces of pedestrians that you have in this image data. The question then is, will that affect the accuracy of our training? Will that affect the utility of our recorded video material? My initial assumption here would have been — yes. If I naively train, an image recognition neural network to classify pedestrians for example, it would automatically learn that everything with a blurred area is a pedestrian. Just recently, we have come up with some solutions to this. But I must admit, I'm not a deep expert in machine learning, to be able to comment how well this actually works. But we might end up being in a situation where we can record the data where we can blur the faces or the license plates. And still this can be utilized for training future systems. This seems to be something that AI researchers are just now starting to tackle.

IEEE IoT Magazine: But let us then look at the following. Let's say you have a GIS system (Geographic Information System), which uses fleets of cars, that look at streets and do photogrammetry. With the miniaturization of the electronics, we see quite a few uses of cars as sensors, where you cooperatively collect data for purposes other than just driving. There seems to be quite a bit of that going on and it seems to have appeal. So, it's maybe the third party stuff that Steve was talking about, and that also seems to be extremely valuable.

Steve Schwinke: I think it's extremely valuable. I've been contacted by companies that build roads, because we have access to all the vehicle data, chassis, data, powertrain data - we might call this pothole data. They want to use our data before and after any improvements. They want to make sure that they're targeting the right roads and the right things for improvement. This will help us identify where we need improvements on our roadways. After they make the improvement, they want to monitor what happened and we are seeing the popularity of that type of application. There's a lot of goodness around the use of that data just to help identify problematic areas on our roadways today. I thought that was insightful. A company that builds roads is trying to understand how this available data, from cars and buses and trucks, can be used for safety. I keep going back to this: you can't manage it if you can't measure it. I like what Frank said about AI. One caution is that the industry as a whole over emphasizes on false negatives. What I mean by that is, they want to be absolutely certain before they automatically brake a vehicle or try to steer a vehicle back into the lane. Or if they think that they must apply the brakes, because of a small child in the wrong place, one must worry how these systems will operate? Braking, taking control of the vehicle, they don't do lightly, because the last thing you want to do is deploy an airbag when you're not certain that an airbag deployment is necessary. So, the number of false negatives matters. Mary Lynn went over this, but the OEMs over index not to deploy, and that's why they miss certain events. Maybe better access to data to better train in these situations is important. There are solutions, and I am sure we'll eventually get there, in the increase or decrease of the number of false positives, but then also a decrease in the number of false negatives. I know this firsthand that the OEMs don't like to apply brakes unless they're 100% sure that its necessary. And that means that they sometimes miss events that could have been lifesaving.

IEEE IoT Magazine: As electric vehicles (EVs) take a larger share of the global market and require different ecosystems, what impact does this have on privacy, trust, reputation, and other intrinsic requirements? In posing this question we may consider something like the charging of an electric vehicle. When it's plugged in, it looks like a very opportune time to take a look at the vehicle data, what it's doing, what condition it's in. So, all of a sudden, the whole infrastructure we have today of gas stations, looks completely different. It has to have additional functions that we haven't had in the past. When you put that plug into a socket, you want it electrically connected to the rest of the vehicle, it almost begs itself to the to have you do that and look at the data. So, let's talk a little bit about the world of electric vehicles and how it affects the issues we're talking about.

Biplab Sikdar: I think, like you mentioned, when you have to plug in a vehicle to charge it, that presents a wonderful opportunity to pull out all the data from it to look at its past history and so on. What's also important is the fact that the vehicle is connected to the grid. That grid can be either the electrical grid or the information grid. This makes it a little bit easier to track the behavioral patterns of the user a little bit more. Also, I think, more from the point of view of infrastructure, that needs a lot more investment. This is especially true in a city like Singapore, where I am, and where most people tend to live in apartments, I think 80% of the population lives in apartments. This has led to a significant change in policies in the government as to where, the charging stations need to be put up, and what kind of information they can collect. So, going forward, I think this would, of course, lead to a significant change in the way we are able to track the behavior of the drivers and their patterns and the impact it has on privacy. So that's something we will have to have to worry about.

Mary Lynn Buonarosa: Yes, agreed. I'm working on a small study right now looking at charging behavior, where and when people charge their EVs. Some people are still asking the questions about how stable the grid is. Ann Arbor is a place where you'll find a significant number of EVs and people are charging at home, at the University, and throughout the city. The number of charging locations will only increase over time. I don't know of people that are dealing with the issues around privacy. As you well know, but haven't mentioned, when you're plugged in is there the opportunity to get a lot of data that people don't necessarily have to share. Is there a way that we can charge anonymously? I really don't know, who was addressing those data privacy issues!

IEEE IoT Magazine: But you know, the question is, if someone is charging, the charging stations can identify the vehicle, and they know who it belongs to. Do we even need a credit card and have to swipe it? Or is this all automated part of the charging system?

Mary Lynn Buonarosa: Is that what I'm signing up to as an EV Owner? Right, that you can have access to all my data. You know, I don't think most people are ready for that. But you know, if from among this panel, there are people aware of who is working on the charging and privacy issues it would be good to address this. It strikes me that a lot of people are working on these issues. Thank you!

Frank Kargl: I don't know how much time we have today. But I can tell you an interesting story on this. This was almost

10 years ago, when the ISO SAE 1511-8 standard was being drafted (https://en.wikipedia.org/wiki/ISO_15118). It basically controls how a car talks to the charging station and to the grid and implements or enables the plug in charging systems that we would like to have. Back then a good friend of mine approached me, he was a member of that IEEE working group and had an intermediate draft of the second version of the NHTSA CAFE Standards (https://en.wikipedia.org/wiki/Corporate_average_fuel_economy). He then asked me, "Hey, Frank, you are working on privacy in automotive systems, can you have a look at this" because there was basically one section on privacy in the draft, which consisted of just two bullets, like privacy is important, and everything should be encrypted, and that was it! Right. He approached me with the concern if this could be used for tracking drivers, etc. What we did back then was to engineer a protocol completely to be fully privacy preserving to a point where we even had a formal proof. We use a model checking tool to prove that the system could not track people anymore, while at the same time still allowing plug-in charging and full system functionality. With that we approached industry suppliers, like Bosch and others, but also the IEEE working group. When we talked to them and we said, "Well, you know, you could have this fully privacy preserving variant of your protocol, you just have to add group signatures and attribute based credentials and some other stuff." Their response was that it's too complicated. However, they accepted that in our analysis, we found that they their protocol was overly redundant with communicating data. They made some of the changes to simply throw out unnecessary data that nobody needed. I think you can have such incremental changes. If you really expect to, as an academic to change the world with your research, there are a lot of obstacles you must overcome. But technically, it was possible to have a protocol that completely removes the opportunity for tracking the drivers. There is a big gap between what is technically feasible and what the world is ready for.

Steve Schwinke: Yeah, I agree. I'm going to move away from the retail owner to the smart grid benefits. And let me give you an example of a couple of companies that we're working with, not in the US. One is doing an electric scooter. And they're using connected vehicle data to understand the charging behaviors of their customers and are realizing that they might have oversized the battery. They're looking at a major opportunity to reduce the size of the battery. That insight comes through connectivity. It's specific information about how customers use and how they charge their vehicle and what size battery do they really need. The other example that I have is a really exciting company we're working with called e.Go Mobile (https://en.wikipedia.org/wiki/E.GO_Mobile) that is redefining the way urban transportation takes place. They're launching in European cities, where they built a car mostly as a shareable vehicle in urban markets, and it comes with a much smaller battery. When you're in an urban environment, it's no longer about how can I get 300 or 400 miles on a single charge. This is meant for a much shorter range, which means that the battery is smaller and costs less. It's designed to move people around, with a shared vehicle option, in European cities, which is really exciting. They have to understand how these shared vehicles are going to be used by their customers, and what are the charging profiles look like. They need to know what the charge level on these vehicles are at any time. When they know, then they can suggest the right match for the customer. This means a vehicle that will satisfy the requirement so a customer can get from point A to point B without having to recharge. This is where this kind of activity is really just going, it's not just about transitioning to EVs. It's about transitioning to reduce the number of vehicle parking spaces too. I'm sure we all know about parking problems, the more we can share these vehicles, especially in urban markets, the better the impact. We know, if the vehicles are electric, they going to create a much smarter city, a much more desirable city and reduce parking problems as well. It's all because the manufacturers get that feedback as to how to optimize the product for the market in which they're operating. That was a long answer but it's important. I get really excited about the other benefits around connectivity as we transition to EVs and sharing.

Biplab Sikdar: Yes, I think since we are in a high density city and we are fairly small, like 40 kilometers wide, some of the problems are simpler in the sense that a single charge can probably last you through a whole day. I think the kind of charging patterns that you might see in a small city like Singapore might be a little bit different from other countries. There is still quite a lot of personal information that can still be gleaned by looking at your charging data: where you charge, how often you charge, and how much you charge. There are some common things that will be there. There are also certain unique things that come from being in a small place with a limited ability to drive around.

IEEE IoT Magazine: As automated driving technologies advance, what roles do you see connectivity play in the future of the Internet of Vehicles — in particular, infotainment, teleoperation, assisting self-driving capabilities, vehicle security mitigation, vehicle diagnosis and maintenance, roadside assistance, user experience, and others?

Frank Kargl: I fully agree to everything you said. You already had a very exhaustive list of where connectivity would benefit automated driving. Maybe I can extend on one aspect. I think cooperative perception and cooperative driving will become a very important feature that has the potential to turn the way we perceive our traffic systems today upside down. Today we basically assume that certain traffic signs play a certain role in how vehicles behave, and they are there because car drivers or the vehicles cannot communicate with each other. There are other ways you could organize intersections if everyone could talk to each other. If there would be a central intersection controller that could tell you that you can now go turn right, turn left, or drive straight, it would look totally different from what we have today. Of course, there is a transition period with mixed traffic where this might not work. But in the long run, this has the potential to completely change our traffic systems in a fundamental way.

Biplab Sikdar: So, continuing with what Frank mentioned. It will change a lot of the way our transportation works. I think it will also have the potential to change our land utilization, especially from the point of view of Singapore where space is limited. For example, if I can ensure that vehicles will always stay in their lanes, then the lanes can be narrower, and so can the roads. And that frees up quite a bit of the land for non-transportation use. So right now, before you can buy a car, you must pay for a 10-year permit, which costs about $75,000. One of the reasons for doing this is to limit the number of vehicles. One reason you want to limit the number of vehicles is you want to limit the amount of surface area you devote to roadways. So again, with connected vehicles, hopefully with autonomous vehicles that are connected, if they are much safer and can operate with smaller lanes there is a knock-on effect in terms of the livability and land use and so on. Maybe I went off in a bit of a tangent, but the point is that this has additional value beyond just transportation, it can also have an effect on how we live.

Mary Lynn Buonarosa: Yes, we know that intersections tend to be dangerous places. I think that cooperative, perception systems installed at intersections will certainly increase safely. But besides intersections, if vehicles are connected and able to communicate wirelessly with each other, for example, if they could broadcast a basic safety message, which includes their location, (their GPS coordinates), their heading and their speed at 10 hertz, then we can also increase safety outside an intersection. As an example, we think that it should be connected and automated. For example, in 2016, there was a fatal undercarriage crash involving a Tesla and a tractor-trailer truck in Florida. I remember thinking at the time, that the Tesla was possibly on autopilot mode before the crash, and it's unclear what the driver was or was not doing. I remember reading about this crash and thinking that had they been connected, there could have been an intervention. That Tesla car could have begun braking to avoid colliding with the trailer because the Tesla would have known exactly where the truck was and where it was heading. And vice versa the tractor trailer could also have acted, so I think outside even outside of intersections, communication has a lot to contribute to safety.

Steve Schwinke: Yeah, I think of an ideal world with a fully autonomous solution. But everything's autonomous is probably much easier than the path we must take which is a mix. You start having some semi-automated and Level-4 cars, all sharing the roads with human beings and imperfect driving behavior. So how do we get there? I agree with Marilyn, I think you must start somewhere. So, start with intersections, signal phase and timing data, and basic safety messages, and quickly legislate. I think, you're going to have vehicles that don't have these solutions, so let's as quickly as we can get all vehicles to include these capabilities so that we can start reducing fatalities. When it comes to semi-automated driving, Mary Lynn brought up the 2016 crash. I look at what GM has done around Super Cruise, when they get to Level-3 driving automation, where they're trying to make sure that the driver is still paying attention. It's not just hands on the wheel, but it's tracking the eyes. If they determined that the driver is inattentive, they pull the vehicle to the side of the road eventually, and then they use connectivity — OnStar — to see if there is something wrong with the driver. They disable the vehicle from automated driving and use connectivity to figure out what the situation is. So, connectivity plays a key role in everything that you just mentioned before. Even at Level 4, you're using connectivity. When a vehicle gets stuck because it encounters a situation that it has not seen before, they use connectivity to sense what's going on around them with cameras and then make decisions on how to get out of this situation. But now that dovetails into the need for a good quality of service, too. Because sometimes that situation is going to happen when the baseball game is letting out and everyone's on their cell phones, while you're relying on connectivity to get the signal back to the people that can actually decide on what needs to take place. It's the kind of activity that will need high reliability and a good quality of service, which is key.

IEEE IoT Magazine: Today, much of the intelligence (driving functions, software, and hardware) is on the vehicle. The ubiquity of vehicle connectivity may enable some driving intelligence to be offloaded to the cloud or edge computing systems. We are seeing precursors of this already such as vehicle teleoperation systems and applications. Where do you see such distributed functionality and architecture in the future? As an example, previously we mentioned intersections, where there might be a central function at the intersection that calculates who can go next. We are looking for your thoughts on how much intelligence can be moved somewhere than the car itself and how does that affect the main issues that we're looking?

Frank Kargl: I can come back to the European Research Project I mentioned previously (Horizons-Connect). We are investigating the concept of digital twins in edge computing devices. The idea is that we could offload some of the processing to a central or non-central edge computing system. This would obviously raise questions of security and privacy. If things that would normally happen locally in your vehicle would suddenly happen on some central device, there would be a lot of opportunities on the other side for creating value. For example, if you have a cooperative intersection and your digital twin could participate in negotiation with the others in determining the right of way, without having to communicate with the real car, that would be quite beneficial. We are looking into this. The project also involves Intel in running the systems in a Trusted Execution Environment, so that you can, on the one hand, do the offloading, and on the other hand, have your data and yur processing protected from the host computer.

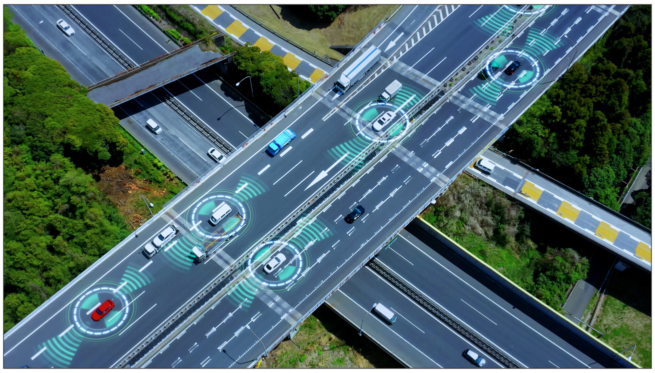
IEEE IoT Magazine: So, are you looking at using homomorphic encryption or multi party process computing or raw differential privacy? I mean, what are the techniques that you're using for that to do the isolation?

Frank Kargl: For the isolation itself, we are looking into Trusted Execution Environments like Intel SGX, so that you have the host security mechanisms that would shield your processing enclaves on the outer host. We have also done other projects which use different mechanisms. But in this project, we are not looking, for example, at secure multi-party computation, which could be an alternative way where multiple vehicles could, for example, engage in calculating right of way or some other functions without revealing their initial input data. But this is outside of the scope of the particular project.

Mary Lynn Buonarosa: What we're doing in the smart intersections project, is that at each intersection, there will be a cooperative perception system (either cameras or lidar), an edge computing device and a C-V2X roadside unit. Based on vehicles and pedestrians seen in the intersection, algorithms running on edge computing devices will, generate data sharing messages, and then broadcast the messages through the roadside unit. These data are stored in the cloud, where other processing could happen. Again, this is a research and development project. We're not actually collecting onboard vehicle data, other than what we mentioned.

Biplab Sikdar: I do feel that edge computing would play an increasing role in vehicle related applications. This is because of latency and computational load requirements, and real time constraints. However, I do feel that, except for the scenario such as an intersection, where you can put sensors, most of the data still needs to come from the vehicles themselves. So, there has to be quite a bit of transmission of data from the vehicles to the roadside units or the edge compute devices. Again, this would also come with the usual considerations about how much you can trust the edge compute devices, be sure your data would not be shared or misused and things like that. Edge computing would definitely play a big role in this, but the data would come from the vehicles to a large extent.

Steve Schwinke: Let me bring this back to a very near-term problem that we see in terms of edge versus cloud. There's not enough processing power on a lot of vehicles and that will be true even for the next few years. What we've been working on with our customers is really cloud computing, but in a smart way. You start thinking about prognostics, as an example, to predict failure or root causes. You begin by collecting data in an unsupervised way through a machine learning models where you cast a wide net to look at how a vehicle is performing and what different things can cause a potential future failure of the vehicle's systems. If we can sample a small number of vehicles with a large amount of data, then we can start training our machine learning algorithms in the cloud to be focused on only collecting the most meaningful and impactful data. It helps reduce data transport costs for trying to do predictive failures analysis for vehicles, but in a way where we're have matured that model and actually minimizing transport costs, I would love to be able to see that model be applied on the vehicle itself, but generally, what we're dealing with here are tradeoffs between how much money you are investing in the processing power in the cloud and the processing power on the vehicle. How much money goes on embedded systems and how much you put on your High Performance Computing (HPC) on the vehicle, versus how much it costs to do the wireless transport and cloud computation for the same things. I do see eventually the shift to do prognostics, and things like that. But for active safety off board, a lot less likely until we fix guaranteed quality of service. Like I said before, the OEMs are not doing too much in the cloud on Level-4 vehicles.



IEEE IoT Magazine: Vehicle communications offer new vectors that may compromise vehicle or user privacy. What do you see as the main privacy concerns related to vehicle communications by both OEMs and vehicle operators? How do you think such privacy concerns should be addressed?

Biplab Sikdar: In terms of security and privacy concerns, we have three things that I can think of. One is privacy of the data itself. For example, what are your sensor values? What are the things you're looking at? How do I make sure that my data itself is secure? Then the second issue is location privacy? How do I ensure that you know where I am? What are my destinations, and my start and end points? What is the exact path I take? How is that data preserved? That's all about location privacy. The third one is identity privacy. This would probably map back to situations where maybe when I'm broadcasting messages related to safety, you can track me over time. Or maybe even when I plug into a charging station to charge my vehicle, then my identity might be revealed. So, there are these three broad aspects of data privacy, location, privacy, and identity of the of the user. Then there are other aspects in this space. What are the issues related to, let's say, the interaction between the vehicle and pedestrians? Do any of the sensors onboard the vehicle impact the privacy of a bystander or somebody who's just walking along the street? Maybe there are certain circumstances, especially those based on the use of cameras that might be taking in pictures of people on the roadside as another example. So, there are likely issues related to a more complex view that we have to think about.

Frank Kargl: I could only repeat things that have already been said. When we started looking at privacy of connected vehicles in the mid 2000s, location privacy was indeed our main concern. There have since been to a lot of solutions. But on the other hand, I also second what people have said that this ubiquitous deployment of cameras everywhere and a modern car with six or seven cameras pointing in all directions, of course, creates privacy concerns. It's not only that cameras are everywhere now, not only at maybe designated spots, but also that it's not clear who owns these cameras and will record and process the data: is that the vehicle owner, who, for example, has watch mode or guard mode enabled and records a dashcam? Or is the video being directly transferred to Tesla and Tesla has a huge database of basically every public spot? In the end, we have a fundamental question whether there isn't a reasonable expectation of privacy in public spaces or not. And there has been many years since a ruling by the US Supreme Court that this is not what you can expect, if you are in public, you're in public. On the other hand, if you look at the European position in GDPR, it severely constrains who can put up cameras and observe public space and puts limits to data synthesis. This is a fundamental societal discussion. Do we want privacy in public spaces or not?

Steve Schwinke: I am not an expert on what Frank just said. He has got me thinking. But when you talk about compromises, I went quickly to just compromising the security aspect of privacy. We design systems, and we follow a security framework, so that our customers' privacy, and other things can't be compromised. I think in terms of attack vectors, and so what I always encourage people to do for their connected vehicle ecosystem is to look at all the various attack vectors. It can be in the cloud, on the vehicle, and in the data transport. So, you have to think about all those different aspects and other attack vectors because ultimately, bad actors will use the path of least resistance. I always think of the On-Board Unit (OBD). An example is the dongle that goes in the little port in the vehicle, where people sometimes plug in insurance monitoring devices, and things like that. The providers don't understand that this now becomes a major security vulnerability or a privacy issue for their customer. You have to think of this very holistically and think of where that attack can come from, and make sure that you design your ecosystem, to protect all aspects for your customers. Just be mindful that the bad actors are going to find that path of least resistance if you don't secure it.

IEEE IoT Magazine: Trust has been a concern that we often hear from the industry. How much can a vehicle trust the data it receives from other vehicles or the transportation and communication infrastructures? Such trust is especially important for data that will be used to support vehicle safety applications. How should one determine what levels of trust will be adequate? What are the main challenges in achieving adequate trust? What are the right testing regimes?

Frank Kargl: The first thing when talking about trust, which I also had to learn when working with people with a philosophy background, is that we should rather talk about trustworthiness of data not level of trust in the data because trust is a decision you make. You can decide to trust something or not. But you might also have evidence that something is trustworthy or not. This is actually what we try to capture in the technology we develop. You can reason about trustworthiness, you can also model trustworthiness in a complex system, and then take informed decisions based on evidence you have in trust. These days, we talk a lot about zero trust networking architectures, or security architectures. The core idea is that there is no initial trust. But clearly you must build up trust so that you have to build evidence of trustworthiness so that you can at some point, make a reasonable decision to trust something. The evidence of trustworthiness can come from many sources, such as from the system itself, the reputation of the company that produces the data, or the development process. I think the important thing here is that we have to think about trust in a quantifiable way. In the end, the decisions we take are not just based on our gut feeling, but rather informed decisions based on which information, which data, which other entities to trust or not.

Biplab Sikdar: I think the whole notion of trust and the central entity on which you will base your trust in the system, that is really the key. What is the basis on which you build your trust in the system? Is it something that comes through the backing of the government? Maybe it is the identities as the main source of trust? Is it because a government entity is behind it? Or are you willing to trust private companies to handle this for you? So again, I think from a societal point of view, having lived in the US, as well as in Asia, it seems to me that, people in different parts of the world tend to trust their governments to different extents. Probably, and ultimately, the solution would have some local flavor to it. The key part here is how do you bring in the whole mechanism for trust? Who is the central authority that you're ultimately relying on in the end?

Steve Schwinke: I'm really paying attention to what Frank just said in terms of trustworthiness of data. And it got me thinking, because as I mentioned before, you have to start somewhere. Hopefully, we start with a simple example: signal phase and timing from traffic signals. We need to make sure that we have a trustworthy method to understand what signal is being broadcast. But we're still going to verify. It will be necessary for industry to get to a point where we can assume that the trustworthiness of the data being broadcast for signal phase and timing from the streetlights is going to be secure, it's not going to be compromised, or else it's not going to be used.

IEEE IoT Magazine: If we now apply this thought to vehicles, does there have to be a layer that has a deep identity associated with every communication. Is it necessary to go beyond the infrastructure that we have today? Are we able to pull this off in a way that is formally trustworthy? At the same time, we must worry about public perception of what trust means. If we get in a vehicle, is it going to do something crazy, or do we have the peace of mind that that it can actually get us from here to there?

Steve Schwinke: I'm a firm believer that we always need to do better. So, I'm always on the side of how do we make everything safer? But at the same time, we live in a world of bad actors. We must move forward to reduce the number of fatalities to make everything safer for everybody, but also be cognizant of the fact that these systems can be compromised. The issue then is how do we prevent the compromises so that we're really moving the needle forward!

Mary Lynn Buonarosa: I appreciate passing on the baton. Well, I have so many really good topics we could address here. Before I talk about public perception of trust, I would like to talk about trustworthiness of the data. As was mentioned this is one of the core technical issues. I think that it really does call for rigorous testing and validation, and millions and millions of miles of testing with cars and trucks and experience with these kinds of environments. Maybe as important, we also have to look at the dangerous edge cases. It's not just a matter of driving north and south through Wyoming and Montana. We have examined roadside warning violation, like someone running a red light, or a risky left turn. Mcity (https://mcity.umich.edu/our-work/research/) is doing these kinds of tests, under the direction of Henry Liu, who's the director of Mcity, director of the Center for Connected and Automated Transportation (CCAT) and he's a professor at U-M's College of Engineering. He is also the principal investigator of the Smart Intersections Project (https://www.mlive.com/news/ann-arbor/2021/01/995m-going-to-university-of-michigan-for-20-smart-intersections-in-ann-arbor.html), where he and his team have developed an augmented reality system to test these dangerous edge cases. You can have an actual Autonomous Vehicle (AV) driving on the test track that's in Mcity, with other virtual vehicles, and actual parking environments. That AV can physically be in these dangerous situations (with virtual vehicles), so it's safe, and provides opportunities that simulation doesn't actually provide. That's one important thing that you can do such tests. Mcity has now evolved to Mcity 2.0, where they're opening that Mcity test environment, by using digital twins, so that allows other academic researchers across the US to make use of the facilities for this type of test. Next, moving to public perception of trust. You know, this is a really tricky area. My dad is 89 and he recently said to me, "I'll never get in an AV." He is still driving because he doesn't trust the idea and so there are generational issues of course, I think a 20-year old will be more inclined to get into an AV even at higher speeds than then maybe somebody's dad so there's a lot of public education that needs to accompany how safe and reliable these vehicles will be. I don't think they're there yet. But I think there is a very big public education piece to be realized.

Steve Schwinke: It's interesting at Ross School of Business, we were talking with people about trust in autonomous vehicles. It turns out that some elderly people were actually more inclined to ride an autonomous vehicle than they were an Uber because they didn't trust the human driver, which I found very interesting. They were excited because it gave them freedom as they started to lose their ability to drive or felt uncomfortable driving, but they didn't necessarily trust a stranger to ride with. There was this dichotomy of do I trust autonomy, or do I trust another person, which I found fascinating. I love what Mcity is doing - I just think of the unprotected left turns that you have heard about from Mary Lynn. The first time I rode in an autonomous vehicle in San Francisco, another driver pulled too far up into the intersection, the AV just stopped because we were both making unprotected left-hand turns. It wasn't the AV's fault; it was the other driver that moved too far into the intersection before they were going to complete their left-hand turns. The AV had to make a complex left turn to get around the car that had pulled up too far, which are the types of things that you're doing there at Mcity through augmented reality, to figure out those the situations and what can be done about them.

Mary Lynn Buonarosa: You raise a really good point and I'll finish with this. You said before, we're going to be driving in mixed traffic that consists of manual driving, various levels of automation, and fully automated vehicles for quite some time. While the AV may behave properly, here's a case where a human driver may err. These are hard problems that will need to be sorted out.

IEEE IoT Magazine: You bring up a key point because we do have 42,000 fatalities in the US, and they speak to the errors of judgments by human beings. The question then is, what is the appropriate bar where autonomy crosses the threshold of acceptability? Is it that it does better than human drivers as opposed to doing something absolute and eliminating all accidents? There is some implicit assumption here that eventually AVs will in fact, be better.

Mary Lynn Buonarosa: Yes, that's what I raised with my dad. Today, people drive and 42,000 people are dead, many more with lifelong injuries, back injuries, neck injuries, etc. While they didn't die, they sustained lifelong impairments, and we can do better. I think there are a lot of dimensions to this, and I think it's going to take a while to get there.

IEEE IoT Magazine: The next question has to do with security challenges and solutions. Connected and automated vehicles must be highly secure as any compromise could lead to deadly consequences. Solutions may require significantly different approaches than handling similar events in enterprise or personal networks. For example, security for vehicles must be handled while taking vehicle safety into consideration. There are many other similar examples that may lead to competing requirements. What do you see as the main security challenges for connected and automated vehicles? What's the state of the art of current solutions considering all those different requirements we may have?

Frank Kargl: Okay, one aspect of security that comes to people's mind first is, of course, securing the vehicle from infiltration. You don't want the vehicle to be hacked. This is something that industry invests a lot of energy on. For quite some years now, many of my former students work in industry for companies like BMW or other places, trying to integrate security mechanisms into cars. When it comes to automated vehicles, however, there is one new aspect to it, and that's securing the control processes. We have complex algorithms that rely on inputs that then produce outputs to tell the vehicle where to drive. These processes can be manipulated by manipulating input data, or maybe if we have infiltrated the vehicle, by injecting messages to campus at satellite and wanting to flee, you want these controlled processes to be safe, and non-manipulable by malicious entities. This is something where a lot of research has gone into that suggests the state of the art is not in practice to address this challenge. And this can mean sensor security, or machine learning systems that detect objects, or control algorithms for platooning, or many other things. This is a fundamentally new aspect that needs to be addressed.

Biplab Sikdar: I think Frank touched on most of the important stuff here. The other issue is securing the AI and machine learning algorithms that will play an increasing role in autonomous vehicles in the future. This includes securing the algorithms against data poisoning attacks, making sure that they're secure against adversarial examples, and so on. This will play an increasingly important role in the future. I think this is something that is still to a large extent an open problem.

IEEE IoT Magazine: If we were to look at published numbers, a typical automobile today has anything from 150 to 200 million lines of code. We don't know whether that's correct or not so Steve Schwinke may have a comment on the numbers. But those are the kinds of numbers we've seen circulating in quite a few places. That's a tremendous body of software on each vehicle. If we were to look at supply chains for software, the ability to test all that software it's a stretch of the imagination that such a larger body can be delivered without bugs built into it, and that's without even achieving Level 5 autonomy.

Biplab Sikdar: Yeah, absolutely. So as things get more and more complex, definitely there will be bugs in there, that we will not be aware of, and they are just waiting for somebody to discover them and then maybe figure out a way to exploit them.

Steve Schwinke: I'd say when someone says that software is done, you know it's never done! I mean, this is what we do at Sibros. We provide a platform to update everything within the vehicle, and we do it in a way to update anything that is flashable. But before we even start to design this system, security and automotive safety came hand in hand because those words do become interchangeable. That's why we're ACLD (Adults & Children with Learning & Developmental Disabilities) compliant, when we provide SOP (Standard Operating Procedure) updates, and that's why we follow what's known as the Bob Kane security framework. I'm really proud of the work that was done to put it together, because it really did bring in a lot of automotive, a lot of cloud to develop a security framework that addressed all the various attack vectors from arbitrary software attacks, and rollback tags and Eavesdropping attacks. All these vulnerabilities are taken into consideration when building that framework for deploying new software for the vehicle. Ultimately, they're going to attack the weakest part of that ecosystem, whether it's in the cloud, along the transport, on the vehicle itself. That's why you should take everything into consideration. And then on the automotive side, which I'm proud of, about six years ago, you started to see gateways going into vehicles. And these are, what the former GM dirty guy would call the clean side and the dirty side of the vehicle. So, you have the connected side of the vehicle where the telematics and infotainment systems ran, and then you had a gateway, that was also a switch that really limited access to the driving functions of the vehicle. And we're seeing the adoption of gateways pretty much with every automotive product today where there's a lot more isolation that must take place between connected and the act of driving a vehicle. And, you know, companies like NXP build the ESP 32 G, they're really doing a great job of making sure that these gateways can protect the safety of the vehicle.

Mary Lynn Buonarosa: In terms of what we deploy in Ann Arbor, we have a production security credential management system (SCMS). All the device manufacturers, that we're deploying in this environment, must attest to cybersecurity safety features to enroll their devices in the SCMS. Every message that is broadcast is wrapped in a security layer, so that a receiving device knows that it can trust the message. We have also done work and are continuing to do work on misbehavior detection. If a device is hacked or vehicles are spoofed, and there are ghost locations being broadcast into the environment, you can imagine that could create crashes by vehicles receiving a message indicating there's a vehicle that's overlapping. There are algorithms to detect these bad actors, then report to a central authority to have their credentials revoked.

Acknowledgement: We would like to thank Dejan Milojicic, from Hewlett Packard Labs, for pioneering the format for Virtual Roundtables in *IEEE Computer Magazine*, and to Rath Vanithamby, the *IEEE IoT Magazine* Editor-in-Chief for encouraging the inclusion of such material.