FTC Connected Cars Workshop: Privacy, Security Issues Related to Connected, Automated Vehicles
June 28, 2017
Segment 3
Transcript

SPEAKER 1: [INAUDIBLE] sorry.

KAREN JAGLELSKI: Here we go. [INAUDIBLE] no, it's not. It's panel two.

KAREN JAGLELSKI: And she also is the author of this amazing infographics that was outside and apparently has gone-- I've been told has gone [INAUDIBLE]. So anyway-- so thank you so much and thank you all for joining us. And we're going to start questions with you, Dr. Pajic. So we heard Nat Beuse from NHTSA talk about the attack vectors present in modern day vehicles. But who are the attackers and who is it exactly that we're worried about?

MIROSLAV PAJIC: Well, first of all, thanks a lot for organizing this and I'm very happy to be here. So I would like to start with a [INAUDIBLE], but pretty much who isn't. From a few years ago when a group of grad students was able to hack into a car and show how if you get access to the OBD port, you can easily attack the vehicle.

Or if you mess up with the meta data on a CD drive, you can actually also take over the car completely. Then it was like, OK, if you just have physical access, you can access-- you can compromise the vehicle. Then it was easily shown how you can do that over the air.

So pretty much we do have from one side a standard threat of hobbyists who are doing that for whatever particular reasons. But we also have a way more serious situation where imagine if you find zero day exploit in most of the vehicles manufactured by one manufacturer or one of the OEMs. You would pretty much be able to launch a large scale attack and take over control over hundreds of thousands of vehicles at the same time.

So you do have this problem of security in vehicles also as a part of the national security efforts to address. And one thing that a lot of us don't want to directly admit when it's related to the security research, but we've seen in other domains people selling zero day exploits to other companies and people with financial interests that then would hedge thedon't(n)-10(C [(hundr)3(e) t)-2ins.24 (

detection and monitoring. Argus also offers such products and services. So you know, maybe there's the first attack.

If we take a center for Disease Control type of mentality, there's patient zero and maybe patient two or three. But then we detect that campaign and we can immunize. So even if there's a how to manual, we have a how to manual as well, and w t

SYED HOSAIN: I think one of the things we need to be careful of is to recognize that it is not the security aspect of the vehicle that we're talking about here. It is also the fact that it is the analysis of the consequence of a breach that matters, OK? So if you just knee jerk react and say everything nee

thing which is, I think, very important is to try and recognize that there are-- for large scale attacks, there's only a certain amount of points of contact, if you will, to the vehicle-- long range contact, either satellite or cellular. And therefore, if you can start building in all of the protection over there as much as possible and then reduce the likelihood of an attack getting through to the systems behind that point, you're going to do a better job.

And so they're recognizing that that's the point of-- where most effort is being placed today. On the other hand, individual changes to systems within the car for even a legitimate update of a functionality feature in the car needs to be thought through. There are complex systems that are growing up around this place.

DAVID SCHWEITERT: And Karen, I might add, I mean, obviously it's very dynamic as it relates to what we are facing in terms of cybersecurity. I mean, obviously, between threat vectors, I mean, the instances that the auto sector is facing aren't all that different from other industries. I mean, it's not so much that we have a particular threat vector against us. It's that, you know, manufacturers are increasingly using multiple layers, whether it's production, security by design, manufacturing updates, and then post-production fixes to try to address some of the things and the vulnerabilities. I think Syed and others referenced earlier that nobody's expecting or selling a vehicle believing that it's going be perfect forever.

But I think it really goes back to what Jeff [INAUDIBLE] earlier during his keynote as well as Nat from NHTSA were referencing is the whole generation of additional technologies that are being added to vehicles aren't being added arbitrarily. They're being added because they provide an overall benefit in some way, shape, or form.

So for consumers, that impacts people directly. It could be some of the conveniences that were referenced as it relates to remote start or remote lock, unlock, and that type of thing. But at the end of the day, it also goes back to vehicle functionality, which obviously then relates back to the benefit that the driver or the user experiences.

And it really gets back to some of the statistics that Nat and others were speaking to that in the past, in a traditional vehicle context, really weren't things that automakers, let alone regulators, could really wrap their arms around because they just weren't possible and, you know, the average age of a vehicle on the road is now about 11 and 1/2 years and the vehicles are getting more and more complex. But that's not necessarily a bad thing, and we're going to get into it as it relates to what that means for recalls and consumer impacts. Certainly there are cybersecurity challenges but it's a very dynamic process.

Obviously, there's been a lot that's been done by OEMs and suppliers in the larger ecosystem that will get us to the point where we're staying a step ahead. Does it mean it's perfect? No, but there's a lot of development that's ongoing, some of which I think is directly related to the fact that there hasn't been a commercial hack of a motor vehicle, partly due to some of the efforts that are being taken by the industry and our members.

Some of that relates to kind of the forward leaning aspects of the auto ISAC, which is obviously a component of the larger ecosystem. But you know, whether it's the security by design, some of

the standard setting bodies, whether it's SEE, ISO, some of these collaborative engagements that

machine learning can make these systems safer over the long run. And so how we approach some of these standard privacy principles may wind up needing to be a little bit different in the car space.

SYED HOSAIN: Yeah, just one observation I'd like to make which I'm hoping people will appreciate. Physics gets in your way. If you're assuming that autonomous vehicles will be run

because, yes, it will create a bottleneck and no vehicles will pass there. But what if you are in certain nicely crafted messages?

And those are kind of things-- those are the networking attacks that are now used. With connected cars, the next step is coordination between them. And once you start messing up with the information on which you base the coordination between vehicles, you actually have a lot of calls.

MARC ROTENBERG: I just wanted--

KAREN JAGLELSKI: [INAUDIBLE] oh, OK. You've got enough questions. OK, Marc.

MARC ROTENBERG: Well, I just wanted to respond to Syed. I'm not quite as sure as he is that there isn't a scenario for remotely operated vehicles. We've done a lot of work over the last few years concerning drones, which are remotely operated, unmanned vehicles.

And the intent, of course, is to deploy drones in the national airspace. And there are lots of scenarios under which drones collide, drones crash, drones fall to the ground. And even to pick up on Meg's phrase, the failsafe scenario for a drone, which is to return to waypoint doesn't work if the drone's battery has been diminished and it doesn't have the energy to return to the waypoint.

So I think there is at least some value in trying to look at some similar regulatory challenges anticipating what some of the risks might be. Miroslav mentioned GPS, for example. The GPS signal is not encrypted, so of course, spoofing a GPS signal is not a difficult thing to do. And there are some security measures that are taken, but there are also a lot of attack scenarios that are based on sending a vehicle or a drone to a different location.

KAREN Jo11(e a >>BD o)-4(f)-0.9( )-10.1(at)-5.9(t2 -2.]TJ e)4(nt)-15 T5hkOht

MEG NOVACEK: First thing is there's 50 to 100 computers in a car. So that's number one. The complexity is just so much higher than IoT. Two is the lifespan. The 11 and 1/2 year life that people expect is another huge challenge. So having a system that can be updated, whether it's technology updates or security updates, is going to be a huge-- is a huge challenge for the community.

KAREN JAGLELSKI: And part of it is historically, consumers don't bring in their cars for recalls. A friend of mine has three open recalls that she really needs to get fixed. So how realistic are over the air updates at some point?

How can we address that issue of-- I forget the percentage. My friends at NHTSA know better than I do. But it's-- Dave, you know.

DAVID SCHWEITERT: Yeah, I mean, I don't want to jump in if anybody else wants to answer. I mean, if you look at recalls generally, so holistically, recall participation rates vary. The longer a recall on a vehicle is open, the longer it takes to remedy.

NHTSA, I believe, the statistics are at around maybe 72% on average as far as recall participation, and recalls run the gamut. It can be everything from a decal that needs to be updated to something like an airbag, which some of us have experienced firsthand. And that gets back to what I was alluding to earlier as it relates to increased technology. We believe from a manufacturing standpoint that technology being added to a vehicle not only helps as far as the vehicle performance, but it also helps the manufacturer as far as lessons learned, things that can be repaired ahead of time.

MEG NOVACEK: There's several companies doing it today, and there's a lot of development for the rest of the companies to go that direction. So I can't state what percentage and when we'd all be there, but--

SYED HOSAIN: It's definitely something that is going to happen. One of the things we have to be careful about is right now, the rules for recall are essentially voluntary. If the owner of the car chooses not to do something, as in your friend's case, it doesn't get done.

So there is a question here in my mind. Should an over the air update be forced on a car owner? It's their car. It's their systems.

It's their multiple computers inside their car. If one can provably say this is a safety issue that relates not to their vehicle and their car, but their public presence on the roads, then maybe one could argue that is possible. But I don't think that those rules exist.

I think that's maybe where some of the legislation perhaps needs to be-- that in certain safety related issues beyond the individual owner of the car, there may be a need to be able to do this. But is OTA happening?

We're certainly getting ready for it. There's no doubt about that. And some car manufacturers are doing it already today and others are-- I mean, our systems are designed to allow the car manufacturer to do it. But we have to think through when and how and where and who's giving them the permission to do it, et cetera.

KAREN JAGLELSKI: Meg.

MEG NOVACEK: A couple of things there-- I'm not sure if you'd call in a research group or what, but it's a couple-- you know, at least University of Michigan and New York University are sponsoring a group called Uptane, which is focused on secure over the air updates, and several companies in various roles within the automotive ecosystem are participating in that to make sure that it's a robust approach so that we as a industry can do secure OTA. The other challenge, I think-- I get the idea of a safety or security recall may preempt the driver buy-in or the owner buy-

the brand reputation, and then the system and the potential exploit. So some of that is happening in real time today as it relates to the auto ISAC, which our association and others have stood up, which includes not only manufacturers but tier one, tier two suppliers.

And one of the mechanisms there is to ensure that information is shared across the platform to ensure that others can learn from what may be playing out in real time. So you know, it's going to differ. I think, you know, would some say, well, one manufacturer is going to make a decision differently than another? Absolutely. It depends on what their overall design decisions are and how they factored it in.

ALLAIN SHEER: Does it make a difference, though, if the information-- what's at risk is safety as opposed to what's at risk is consumer information that might be stored on the system?

DAVID SCHWEITERT: Oh, absolutely. I'd say that there would-- in that case, I think this is maybe what you're looking for, that there certainly would be a tiered approach in terms of how an OEM would face that type of cyber vulnerability based on their responsibilities with--

ALLAIN SHEER: But what goes into the tier? That's what we're trying--

DAVID SCHWEITERT: And I-- you know, representing an association, I can't give you a definitive as it relates to what one OEM would or wouldn't do, nor would, I think, you'd want that shared in this context.

KAREN JAGLELSKI: Meg-- but I think Meg wants to share that with us.

MEG NOVACEK: And it's not OEM specific. It's really a-- I think most of you will be able to relate to it. It's obviously-- well, to me. I'll just say my opinion.

So safety is first. You know, I think if someone is driving-- I'll say if I'm driving in a car and my safety is at risk or my privacy and I want some to decide which they're going to handle first, I'm going to vote for my safety every day. That's just my personal preference.

The range of the hack, if it can only be done 10 feet away or i

you know, companies have more than one person working on it, and there's a lot of activity in parallel.

And that's how they're going to prioritize it. The other is what-- so once the experts figure out how to address it, whether it's blocking the vulnerability or remediating the impact, whether or not that solution can be applied to the car as is is another factor. Do they have to change hardware in order to change the software?

Is it a software only? Can be done over the air or does it have to be brought in? All of these things come into account.

And then if the car has to be brought in, again, I'll say it. Myself as a customer? I don't want to have to go in every other day.

So I'm going to want them to bundle the work only if I have to go in. So all of these things are taken into account when companies are figuring out how. Marc?

MARC ROTENBERG: I don't really disagree with Meg about prioritizing safety over privacy. But I do want to point to a very interesting privacy risk that I wish the manufacturers would prioritize, and it has to do with a Bluetooth pairing of cell phones and rental cars. It's almost everybody's experience nowadays that when you rent a car with Bluetooth connectivity and it asks you if you want to enable your cell phone-- which is a safety feature, by the way, because it enables hands free driving, which we should encourage-- it captures your entire contact list and all the rich data associated with that and stores it on the vehicle. Now it would seem to me to be a priority to ensure that after the rental period was over, that data was routinely deleted because the risk of identity theft and financial fraud and a zillion other things seems quite obvious. And my question is, is some progress being made on that particular cyber vulnerability?

MEG NOVACEK: So if I can just butt in here because I don't want to tread on panel three's toes too much because he'll be mad at me. And I would say that the FTC did-- we did issue a consumer and business education piece in this area. I think that's right. For example, my husband bought a used car, and on the car was the previous owner's data. So--

MARC ROTENBERG: But is it the driver's-- see, this is where we get into very interesting, you know, liability allocation issues. Is it the responsibility of the driver to figure out how that data has been downloaded and to subsequently try to delete it, which is not an easy thing to do? Or should it be on the manufacturer, service provider, which it could be a routine procedure to ensure the data is deleted? And I think there are lots of issues that look like this particular one. And it would not be fair to put the responsibility on the driver where the service provider could manage the problem more efficiently.

MEG NOVACEK: I think Peter will be sure to address that issue in panel three. Right, Peter?

DAVID SCHWEITERT: OK.

SPEAKER 2: Me too.

SYED HOSAIN: So two questions that you raised, one of which I think has to do with the fact that how does the OEM know the car got sold. So I don't think you can put the onus on people who actually have no possible way of recognizing when something needs to be done. And you've got to be careful about that.

So where does that answer to that question lie? Maybe all they have to do is make it easier than it is today and let the onus lie on the driver who either purchases or sells-- excuse me, the person who sells the car and says, I'm going to get rid of all my personal data, and go from there. With regards to download of priorities and updates and how often and when you do it, it's a matter of not just doing an update willy-nilly.

I love to draw analogies and I don't know how many people in this room ran Windows 7 systems at their home and woke up one morning and, lo and behold, they were running Windows 10 and it was done without their permission or knowledge. That is the kind of thing that corporations need to avoid. We need to be careful to make it a choice, an informed choice, as best as we can-- and cars are darn complex systems-- as best as we can to make that happen.

So prioritizing the kind of updates that you need to do a car has to be done with a, what's the consequence? You do not want to break a car. PC is easy.

You do not want to break a car. And you've got to be careful that what you're doing hasn't caused some other system, if it is a security or safety system in particular, to have lost its fu

t

SYED HOSAIN: I goes back to the point I made, which is that I think AV vehicles will not be

MARC ROTENBERG: Yes. I mean, I've been at this for a long time, and I think the United States does need a comprehensive approach to data protection that would most certainly include vehicles. I don't think the notice and choice approach which people talk about works at all for privacy protection. I mean, if we're speaking frankly, notice and choice operates really as a disclaimer or a waiver.

It's a company saying, this is what we're going to do with your data if you purchase our vehicle and do business with us. And if you don't like it, don't purchase our vehicle. But you see, that's not privacy protection.

So the way we solve privacy protection is by saying to a company if you choose to collect the data, which is the choice the company makes-- it's not a choice that the individual makes-- you bear the responsibility for the consequences if the data is misused. And I think that is almost always the right approach to privacy protection. It can be technologically neutral. It can be service neutral, and it has also the benefit of encouraging companies to think carefully about whether they really do want to store, for example, unencrypted credit card information. Many companies were doing that until they faced liability and they realized it was not such a good idea and they stopped storing it.

KAREN JAGLELSKI: Lauren?

LAUREN SMITH: Sorry [INAUDIBLE]

SYED HOSAIN: Just a quick--

KAREN JAGLELSKI: [INAUDIBLE]

SYED HOSAIN: Oh, Lauren first?

KAREN JAGLELSKI: Lauren-- Lauren.

LAUREN SMITH: So you know, I think it's important to drive home the point that it's not a wild west when it comes to protection of consumer data. I mean, we have the Federal Trade Commission that has been active in consumer protection around data privacy within the internet of things for years. Cars are not that unique in this particular area, and it sounds like, you know, obviously there's increased interest at the FTC in this growing quantity of data in cars. There's also, you know, self--

DAVID SCHWEITERT: Karen, I know you've got another panel that's really going to focus on this, so I'll just maybe conclude with this point. And you know, if you look at what's happening with the privacy principles, I'd be shocked if there was another industry that has been as forward leaning as the auto sector, both in terms of the privacy principles that Auto Alliance and Global Automakers have charted. I mean, this is something that was effectively hammered out, that it's dynamic. It's not static.

And it is FTC enforceable. So as it relates to something that needs to happen legislatively, I would say it's always important to reiterate to the public that what they may witness either on their internet at home or their personal device is far different than what otherwise is executing in the vehicle. And data-- all data is not created equal.

There's a lot of steps being taken by manufacturers. It's going to vary as far as how they roll it out. But in terms of anonymizing, minimizing, and those type of things, Marc did raise some fair points. But I'd be hard pressed to think of another industry that's been as forward leaning as the autos in terms of how they manage data.

MARC ROTENBERG: Could I make just one point on privacy and innovation?

KAREN JAGLELSKI: No. Hey, I'm telling you. Pater is going to leap across the table and grab you by the neck, but go ahead.

MARC ROTENBERG: This is a good conversation to have, and I know it's a conversation that's taking place across the industry, and we do appreciate it. But in fairness, you know there is a view which says an innovative product is one that maximizes the technology in the public benefit and minimizes the risk to privacy and personal data. And what the GDPR is attempting to do is to reduce the risk of the misuse of personal data.

You can collect endless amounts of emission information, safety information, breaking information, acceleration information. Go for it, right? It's not the case that privacy rules try to restrict data analysis analytics.

It's simply the recognition that there's a certain category of data that really does adversely impact people. It affects their insurance rates, their health payments, their employment opportunities. And if you're gathering that data, then I think there's some responsibility.

ALLAIN SHEER: [INAUDIBLE]

KAREN JAGLELSKI: Sure.

SYED HOSAIN: Very quick. I don't disagree. That's not the point I was trying to make, I guess.

I think the real fundamental flaw that I have of having looked to the basics within the GDPR is the fact that it is being administered by people who don't necessarily understand the intent of what is going to be done, number one. Number two, it's the penalty phase where if you look at

what is required, the companies that matter, the larger corporations to whom it could be a serious issue, are going to think twice, and it's going to slow them down. Is that a good thing?

It could be. I mean, they may think through some of the privacy issues that they should have thought through better. Otherwise, it could be an issue.

ALLAIN SHEER: All right, this is the second question from the audience, and it assumes that there's some kind of certification as to cybersecurity practices. And the question is, wouldn't the automakers simply falsify their cybersecurity data?

KAREN JAGLELSKI: It's from the audience.

MARC ROTENBERG: Is that a real question?

MIROSLAV PAJIC: But I would say so in the example today I guess everybody is suddenly referring to, the falsification of evidence was done to pass the test. But then the car would improve the overall experience of the user. Falsifying security related data would not, at the end result, if there is a vulnerability there, improve safety of-- improve the overall experience of the driver.

So from that perspective, I don't think that there is the same motivation between those things. I think if more goes according to the Meg's comment, it goes to the user standard practices, something that you have in FDA in certification of medical devices or in avionics. So there is a way how you can reason about safety of these very complex systems. I mean, cars are complex, but they're not as complex as Airbuses or Boeings of the world. So we can reason about a security in a similar manner. And there is a push both from academia and industry to build these kind of assurance cases that can be presented to the government and certification authorities to say, yes, we did follow some practices, and we provide some guarantees that security concerns have been addressed.

KAREN JAGLELSKI: All right, well, we're out of time. So I'd like to thank all the panelists and in particular Lauren, who stepped up to the plate. But thank you. All I think it's been very interesting, and we appreciate you being here.

MIROSLAV PAJIC: Thank you very much.

[INAUDIBLE]