Audio file

cyber-security-podcast.mp3

Transcript

00:00:05 Speaker 2

You are listening to the HCL Engineering and R&D Services Podcast powered by CTO Straight Talk.

00:00:13 Speaker 3

Welcome everyone and thank you for joining us today for the third episode in our podcast series on securing the modern vehicle. This series brings together engaging conversations with cyber security thought leaders from HCL Technologies and Cybellum - as we look at the evolving industry challenges, discuss some of the latest security technologies and share insights to stay ahead of emerging cyber threats that are faced by the automotive industry.

00:00:40 Speaker 3

In our last episode, we had an engaging exchange on the era of regulations. We discussed not only policies that have been published to guide the industry, but also how first regulations such as ECEWP 29 will be coming into effect in July of 2022, and what actions manufacturers and suppliers will need to take for compliance.

00:01:05 Speaker 3

And during that exchange it became clear that there will never be a final destination state for cyber security in automotive. SThe industry will continually need to adapt and evolve to vulnerabilities and threats in the complete ecosystem to keep the vehicles secure.

00:01:22 Speaker 3

Which leads us to today's topic evolving automotive cyber security strategies. Hello and welcome. I am Chris Barman, Vice president of strategic initiatives in the Transportation division at HCL Technologies, and I am excited to be the moderator for today's session.

00:01:41 Speaker 3

We're being joined by two esteemed experts in cyber security - Wolfgang Heinrichs is the head of European automotive sales at HCL and we are also joined by Ronen Lago, who is the CEO at Opora IO and an Advisory Board member at Cybellum as well.

00:02:02 Speaker 3

Today's episode will focus on the continuously evolving strategies that are being developed and deployed to maintain vehicle security, and we are fortunate to have Ronen and Wolfgang with us. Wolfgang, Ronen thank you for joining me today and can you please provide a deeper introduction about yourself and your background for our audience? Wolfgang, perhaps you can get us started.

00:02:26 Speaker 4

Thanks a lot Chris for the nice introduction. My name is Wolfgang Heinrichs, I'm within HCL for the last four years.

00:02:34 Speaker 4

My background is electronics and electrical engineering, and I've been involved for more than 30 years now with the automotive industry, especially in developing ECUs and strategies on how all ECUs can communicate with each other, that is all.

00:02:52 Speaker 3

Very good, thanks Wolfgang, and Ronen?

00:02:56 Speaker 5

Yeah, hi Chris, thank you for having us here. So, my name is Ronen. I have a degree in electrical engineering. Started my cyber career 25 years ago, in the intelligence forces of the Israeli army, focusing on critical infrastructure and OT. Finished my PhD in this area. In between I was the CTO for Lockheed Martin dealing with all the Advanced Technologies, Autonomous Vehicles and autonomous something around the world.

00:03:28 Speaker 5

And then I moved. I was the head of security for Daimler. So, I am also coming from the OEM perspective and their challenges.

00:03:35 Speaker 5

And the last year I am back to the startup Arena and I'm supporting startups and having my own startups -mainly around automotive and supporting advisory boards in different areas. I'm happy to be here today.

00:03:53 Speaker 3

Thanks Ronen. Glad that you're here and given your experience, I think you'll have some deep insights to share with us so.

00:04:01 Speaker 3

Now let's talk cyber security.

00:04:04 Speaker 3

So, first question, I have for both of you is in an ideal world automotive OEM's who are pursuing cyber security measures would prefer that it was included within their design of their electrical architectures of their vehicles many years ago. But in many cases those architectures were designed before it was ever really thought of what cyber security would mean in the future, so these legacy designs may provide only a limited opportunity to bring in security measures.

00:04:37 Speaker 3

So how should OEMs and tier ones be thinking about what they can do with their architectures today in order to have efficient and effective strategies on these legacy systems?

00:04:50 Speaker 3

Ronen, maybe you can get us started?

00:04:52 Speaker 5

Yeah, so I will take it from our perspective. So, from the OEM perspective, yes there is some legacy. I think they're understanding now that the problem pf security is not just an IT problem and has also become a safety and reputation problem and needs to be taken care of as they're taking care of other stuff.

00:05:12 Speaker 5

And it's a business risk, not just IT stuff inside ECU.

00:05:16 Speaker 5

So, when they come to this understanding, the old engineering part, and R&D and budget are focusing on 'OK, what can we do next? How can we think forward?' and again we cannot of course cover all the threat scenarios there, but if we were thinking it's only a minor impact on the car or has a minor impact on the company, this mindset has changed and now they're adding more and more capabilities.

00:05:46 Speaker 5

One of them is of course, segregation between areas others are more data encryption and creating trust and another one, like any other product, is software updates because they understand that things will fail, and they may need to fix it. And part of it is so they will be able to fix it in advance.

00:06:06 Speaker 5

So, I think the main mindset that OEMs are taking today is not if they will be hacked or what happened in a specific attack, but what's happening the day after?

00:06:16 Speaker 5

Let's assume you were hacked.

00:06:18 Speaker 5

Is our architecture supporting it? What can we do with it? So the minds have changed to more "how?"

00:06:25 Speaker 5

Kind of business continuity or vehicle continuity after an attack has happened and not just the prevention in advance. And I think this is the biggest change that we see today coming into the architecture planning of the at least the bigger OEMs.

00:06:43 Speaker 5

That's at least from my perspective.

00:06:48 Speaker 4

I can only join what you recently stated. Being tightly connected with the OEM's and what I see is they really are looking to have policies in place first that gives them a little bit of guidance about what to do, when to do how to do, right?

00:07:06 Speaker 4

Besides that, of course they are now implementing a little bit of a cyber security management system to track and trace all these kinds of activities and have documentation readily available to be certified at the end of the day.

00:07:19 Speaker 4

On the other side, going a little bit more into the architecture or the process development cycle of the customers come – yes, as you rightly said, they have two problems.

00:07:31 Speaker 4

On the one hand is the car that is already sold right and needs to be secured in reverse, so to say.

00:07:37 Speaker 4

And the other one is supposed to be launched pretty soon.

00:07:41 Speaker 4

So, these are the challenges if my customers look on to the V cycle, and they even called it today model with like a W rather than a V.

00:07:51 Speaker 4

Because on one hand you must do the engineering portion, which is a little bit on the on the right side of it, right where you must implement all your measures, your activities, your track and trace ability activities to make sure, from an engineering point of view, you try to be as preventive as possible. On the other side you have the right side which is at the end of the day, making sure all the test and integration is being backed up.

00:08:17 Speaker 4

What you try to do on the engineering side on top. There is a lot of activities going on to get this really under control.

00:08:24 Speaker 4

The thing that I recognize is that while vulnerabilities are somehow being under control, it might be too strong a statement, but they have an idea how to do that.

00:08:37 Speaker 4

And, significant area is the threat area, right? Because they need to get ideas - What hackers really do have in mind to manipulate my car.

00:08:48 Speaker 4

And what are the areas of threats and layers or like you say APIs to really get into my car through the centers, through the gateways, through communication from inside to outside and vice versa.

00:09:02 Speaker 4

So, this is where their customers are really busy with, and they seek help from the market.

00:09:08 Speaker 5

It's actually funny that you said. I'm always telling it as a joke, but it was true when I was hired to Daimler from the CEO, Doctor Zetsche, I got to the board and they ask him why you got an Israeli, who is not German speaking? He's not, you know, part of us.

00:09:24 Speaker 5

And he said, because he thinks like a criminal.

00:09:27 Speaker 5

And this was exactly meaning, you know from the good perspective. It was kind of we need someone that, you know, shake our boats - Think differently, think something from the other side and actually being able to challenge our engineers that are amazing.

00:09:45 Speaker 5

But they need some other perspective to look at it, and I think this is exactly the mindset that you know.

00:09:52 Speaker 5

You have also already seen the executive and I always give this example. You know at the beginning I was insulted but I understand how powerful this means, especially to those leaders to understand that they need it.

00:10:07 Speaker 5

So, yeah totally agree with it.

00:10:10 Speaker 4

And then on top, I don't want to stretch it too much, but on top see there is something that the OEM itself can get under control because it's in their role and responsibility on the other side you have the suppliers, right? Who provide you with the ECUs and whatever else components. So, there is something you have under control and something somebody else must get under control, right? now, that's a little bit tricky.

00:10:33 Speaker 5

Yeah, yeah, it's actually bringing a nice, interesting question.

00:10:37 Speaker 5

Who is responsible?

00:10:38 Speaker 5

They all hope that the suppliers will be responsible, but at the end of the day, if I have a malfunction component in my car as the OEM for a moment it's my problem. It's my reputation.

00:10:51 Speaker 5

You know the impact on my business is very big because the market doesn't care about third party suppliers that no one heard about. The news will be BMW was hit by malfunction product.

00:11:05 Speaker 5

And it's also another area that they understand that somehow, it's not, you know, another one's problem? It's also their own problem and they also need to start thinking about it.

00:11:19 Speaker 5

And actually, the supply chain attack vector is one of the hottest topics today in executive management.

00:11:28 Speaker 3

So, Ronen, you know we talked a little bit about legacy architectures, and we know that the industry is also going to, you know, newer types of architectures with a lot of technologies that are coming into play in the vehicles, connectivity, autonomy, electrification.

00:11:48 Speaker 3

As the industry is thinking about those new architectures, what are they using for guiding principles? Is it just the policies and what's coming out as regulation? Or is there a lot broader thought and perspective that's going into it to, you know, "future proof", or try to at least put the robustness into the best that they can, at this point of time, what are what are your thoughts on that Ronen?

00:12:13 Speaker 5

So, I think it's really depending on the OEM themselves and the maturity of them because our multi-level you know like any other area not only in automotive.

00:12:26 Speaker 5

The basic ones are attaching compliance and policies and procedure, but this is just the basic, you know so if you want to do the check box.

00:12:35 Speaker 5

Yes, I have a compliance. It's good and it's very important and it's mandatory, but it's not really security.

00:12:42 Speaker 5

The guidance usually comes out too late. The threat landscape that we talked about before usually changes until they are approved.

00:12:49 Speaker 5

The regulations usually don't force you to put a lot of budget because they understand there is a financial impact behind it.

00:12:56 Speaker 5

So really, true security needs to come with, you know, the layer above.

00:13:02 Speaker 5

OK, we have the guidelines, but how do we actually implement it? How do we actually tailor those processes to my business, to my vehicle, to my architecture?

00:13:11 Speaker 5

How we take you know there is one compliance I will not put the name which give three examples I have faced with few OEM's they just did those three examples, and they think they are compliant, but they forgot that it's just an example and there is a lot of work.

00:13:27 Speaker 5

To do behind it and I think it's good and it's mandatory to have this regulation and compliance, but it's only the tip of the iceberg and most of them need to understand that it's a guidance and they need to expand the scope and not just hug it like this is kind of the Bible for everything.

00:13:50 Speaker 4

Yeah, I fully agree. To be a little bit more technical, what I see what the customers try to do is there isn't significant effort to really have a domain like architecture or zone like architecture going on.

00:14:10 Speaker 4

Because if you see the more functions, you really can get into one of the controllers, the more you reduce the ability that somebody really is able to malfunction.

00:14:23 Speaker 4

Something that is one area. The other thing is looking a little bit to the legacy terms that are already sold out.

00:14:31 Speaker 4

There is no real chance to change the architecture anymore, but here we see an even greater perspective.

00:14:38 Speaker 4

A lot of efforts to have even shielding around the wires.

00:14:43 Speaker 4

Of a car, that means that the wire that goes from the sensor to any of the controllers will be shielded to make sure that nobody really can sniff the communication from the sensor to the controller.

00:14:57 Speaker 4

Even worse, can implant communication into the sensor's communication to the controller to hack the control on the other side.

00:15:06 Speaker 4

So yes, there is a lot of effort and energy going in to really provide architectures are as much secure as possible, but I believe that it's a long way to go, honestly speaking.

00:15:23 Speaker 5

And taking for a moment what we were saying in in the previous attack surface.

00:15:28 Speaker 5

So, there was a lot of, I call it, engineering focus of inside the car. OK, and they are trying to think about it from an engineering perspective. But you know, hacking a specific car from a canvas - It's very challenging – from an attacking perspective there is a what we call external communication with the smart city with the traffic all the issues that need trust.

00:15:55 Speaker 5

This is probably the soul for stomach because there the Clasico engineers have little knowledge because they are not used, and the attack surface is bigger. So, they're all very focused on the inside architecture, which is dramatically important, but in many cases, sometimes there is a feeling that they're missing the train. Because the train for the big threats that are coming from outside is already there and they must take it into consideration otherwise.

00:16:27 Speaker 5

They will be in the same problem they have with the cars that they have released 10 years ago. Same thing.

00:16:33 Speaker 4

Absolutely, and you you're putting it to the point.

00:16:37 Speaker 4

See, we always have hardware versus software, right, at least in the next generation car.

00:16:42 Speaker 4

The software aspect is becoming far more dominant than the hardware aspect, which may be dominant in the legacy style, but as we know the hardware-based security features are almost pretty much more robust than anything you can do based on software security features.

00:17:03 Speaker 4

Yeah, so from our point of view, so to say the objective for an OEM or even for tier-1 at the end of the day should be to leverage hardware-based security features and to whatever is possible, as of today, right?

00:17:18 Speaker 4

And you see, sensors provide crypto processors, HSMS, TPMS, which would be really leveraged for building robust functions or the foundation for the security aspect in a car. That's at least what we believe might be a very good strategy for the market.

00:17:38 Speaker 3

Yeah, I totally agree.

00:17:39 Speaker 3

To jump in and kind of cycle back to something that you both talked about or mentioned separately earlier, and you know that's the role of the tier-1s as part of the partnership in the ecosystem and the lead of the OEMs.

00:17:54 Speaker 3

And we know that the industry is very competitive. But we also know that, you know, everybody needs to collaborate and work together in order to bring together a vehicle so.

00:18:08 Speaker 3

Do you think that it's possible that any of the tier-1s are going to be defining some of the cyber security architectures? Or some of the policies that their competition may need to comply with or understand as part of a service that goes to the OEM's.

00:18:27 Speaker 5

From vision perspective and from OEM perspective, you know, this is the goal, but reality is not there usually because the business impact and the business competition are usually much higher, and I think some of the OEM's understand that they need to build their own kind of envelope or umbrella layer by their own. So doesn't matter what Tier-1 or Tier-2 will plug in.

00:18:56 Speaker 5

Still, they will have a standard and a layer that they will be able to monitor because they understand it.

00:19:04 Speaker 5

Probably there will not be a kind of a real collaboration between those two. I think that where we do see more challenge is again coming back to the V2X issues when you need.

00:19:18 Speaker 5

A data trust before between different cars, different OEMs, different sensors. And then you cannot protect yourself.

00:19:26 Speaker 5

You know in the car, OK, I will protect myself, but I cannot protect my ecosystem.

00:19:31 Speaker 5

And I think these will be the areas that they will be more forced to somehow collaborate. And you know, to be able to talk in more trusted way.

00:19:42 Speaker 5

Because trust of the data will be one of the key capabilities in the autonomous vehicle world, at least from my perspective.

00:19:56 Speaker 4

Yeah, I fully agree with Ronen and luckily, I've been able to speak to some of the tier-1s over the last couple of months and at least what they're telling me is that in the past and it was just a price battle - you have to be the first supplier for the car to be released to the market.

00:20:20 Speaker 4

Right, and it was really a tough price negotiation to become the first supplier.

00:20:26 Speaker 4

And for that car now with the cyber security aspects there is a little bit of a shift in the strategy that we can see. So the Tier 1 supplier really sees its cyber security plans as a possible differentiation.

00:20:50 Speaker 4

That means while of course price is a significantly large topic and as soon as they can provide a real in-depth cyber security plan, implementation, and robustness, they can differentiate immediately against the other Tier-1s in the same arena.

00:21:10 Speaker 4

Take the ECU suppliers as an example, right? On the other side, we can see that even one or the other OEM is tightly looking at what the tier-1 is going to do in terms of cyber security and how they get their products robust.

00:21:29 Speaker 4

And at least I smell, and I hope I'm not wrong that they try even to listen what the Tier-1s are going to do.

00:21:35 Speaker 4

And maybe they even adopt some of their strategies into their overall strategy. That is at least what I can see on the market.

00:21:43 Speaker 3

So, following up on that a little bit, or building on that a little bit Wolfgang, as the cars are being developed and we've talked a lot about strategies. But you know tier-1s also, you know, have to do a lot of development work and the validation work and OEMs at the end of the day have to make sure they feel that the car is robust and secure.

00:22:04 Speaker 3

What are some tools or methodologies that the suppliers and the OEM should be thinking about to help them through that development process to make sure that what they're designing is robust and as they get ready to release it to the market, you know that it meets all the requirements? And then you know you mentioned the W model earlier.

00:22:28 Speaker 3

Once it's released, it doesn't mean it's done anymore.

00:22:31 Speaker 3

There are continuous threats out there, so you know what is your perspective on that Wolfgang?

00:22:37 Speaker 4

Certainly, Chris, automated tools, both the hardware and of course the software components of the business will be key, making sure the vehicle is developed with maximum possible cyber security in mind.

00:22:52 Speaker 4

There is no doubt about that one.

00:22:55 Speaker 4

If you really look at the market you can see a number of software tools for that kind of automation of these processes, right?

00:23:03 Speaker 4

An example of the tools, of course, if you go into threat modeling and there are tools for security vulnerability, scanning tools for software composition analysis. There are tools for pen testing and there might be many, many more that are already on the market.

00:23:24 Speaker 4

At least to me, I have not seen the tools really evolve that much, at least regarding the automotive space, although they are starting to appear step by step, that is a little bit my view. Maybe Ronen you can join that view.

00:23:39 Speaker 4

Maybe you have a different view. What is your perspective?

00:23:44 Speaker 5

Yeah, no. So, I think it's touching on 2 interesting points here and the tools are relevant.

00:23:50 Speaker 5

One, as we said before, and again, it's also going through the W diagram - Is that yes, they will do the maximum they can do to protect themselves with the latest state-of-the-art solution, but they also need

to take what is happening when it's out there, how to monitor it, how to manage it so some of the tool that we classically call it a vulnerability assessment.

00:24:12 Speaker 5

It's not the classic one. The vulnerability assessment should start from early in the design and maybe even 15 years later or 20 years later.

00:24:21 Speaker 5

And this is the mindset that many of them are missing and the other component that again is not started.

00:24:30 Speaker 5

It started in the avionics which I know from Lockheed, and we see some of it coming also to the automotive area.

00:24:36 Speaker 5

Is all the kind of augmented reality testing or digital twin kind of capabilities which actually enable you, first of all, to really test what you have, the communication - does not matter what tool you will use, what simulation you will use, it is always limited because yes, they have the car, they have the physical component.

00:24:57 Speaker 5

And there are a lot of reality gaps that are preventing them from doing a real test. And if the industry will really get to a point that they have a good presentation, let's call it a digital presentation of a vehicle, or for ECU, or doesn't matter, then we will more tools that are relevant for it, much more advanced capabilities.

00:25:22 Speaker 5

It will enable the test to be earlier in the process. In the W, we call it the shift left.

00:25:28 Speaker 5

We want to test this as early as possible because as late as possible there are too many complications and too many integrations, so I think really as we move a lot of the software it also needs to move from the QA and testing perspective, and again getting out from the traditional pen test and scanner tools, to be based on kind of a virtual capability. But again, my opinion.

00:25:58 Speaker 3

Well, I would say it's clear to see that there will be a continually evolving design strategy and executed practices that are needed to keep the vehicle secure.

00:26:09 Speaker 3

And with the implementation of more connectivity, driver assistance, full autonomy, and the need to keep the vehicle secure by following the W model that we spoke about - not only development, but once it's out in the field, how do we keep it secure - is going to be part of the product life cycle.

00:26:28 Speaker 3

And Ronen and Wolfgang, I want to thank you for sharing your perspectives today and your insights.

00:26:35 Speaker 3

You've certainly provided key points to consider regarding evolving security strategies that are happening in the industry.

00:26:44 Speaker 3

But you know, we touched a little bit at the end here, how are OEMs going to manage assessing their software for emerging threats in an efficient and effective manner? Are there approaches such as the digital twin that you talked about running that could be an effective solution to address this?

00:27:01 Speaker 3

So, to the audience, I would like to invite you to join the next session where two new industry experts will discuss digital twins as an enabler to secure the modern vehicle. And until the next episode, I wish you all the best. Thank you.

00:27:15 Speaker 1

Thank you very much.

00:27:16 Speaker 3

Thank you.