Transcript

00:00:01 Speaker 2

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

00:00:09 Speaker 3

Securing the modern vehicle.

00:00:11 Speaker 3

The shift towards software defined vehicles is on one hand, driving New Horizons in customer experience.

00:00:18 Speaker 3

But on the other hand, creating an increase in the opportunity for exposure to cyber threats.

00:00:24 Speaker 3

Automotive OEM's depend on an ecosystem of not only internal product development but also a strong relationship with supplier partners for the components and systems that will ultimately bring together a vehicle.

00:00:37 Speaker 3

And the OEM's have the responsibility to make certain through this complex ecosystem that the vehicle comes together securely.

00:00:46 Speaker 3

Cyber security and auto industry has been mostly guided by policies, but now the landscape is changing with the publication and implementation of EC WP 29 regulations.

00:00:59 Speaker 3

In this series, each episode will feature cyber security thought leaders from HCL and Sibella, who will share their perspectives on the evolving industry challenges.

00:01:09 Speaker 3

We'll discuss the latest security technologies and provide insights to stay ahead of emerging cyber threats being faced by the automotive industry.

00:01:18 Speaker 3

The various episodes will feature deep dives into 4 compelling topics.

00:01:23 Speaker 3

In episode one, we explore how has the risk profile changed with the implementation of advanced technologies and vehicles.

00:01:32 Speaker 3

Episode 2 will focus on what regulations and standards are being introduced to ensure vehicle security and how it will affect OEMs and suppliers.

00:01:42 Speaker 3

In episode 3, the discussion will focus on the need for a comprehensive cybersecurity strategy across the vehicle lifecycle and in the final.

00:01:52 Speaker 3

Episode we delve into how digital twins can assist in strengthening the cyber resilience of the vehicle.

00:02:00 Speaker 3

Hello and welcome everyone.

00:02:02 Speaker 3

I am Chris Berman, the vice President of strategic initiatives in the Transportation division at HCL, and I will be the moderator for today's session.

00:02:12 Speaker 3

I am being joined by two esteemed experts in cybersecurity slab lancman is the co-founder and CEO of Seibel am a company focused on securing products throughout the design, development in into operational use.

00:02:29 Speaker 3

And Prasad Diane Raju is the vice president of research within the engineering and R&D services at HCL Technologies.

00:02:38 Speaker 3

Today's episode will focus on the rising threats faced by the automotive industry and we are privileged to have Slova and Prasad with us.

00:02:48 Speaker 3

Slava and Prasad, can you please provide a further introduction?

00:02:53 Speaker 3

Slava, perhaps you can get us started.

00:02:57 Speaker 4

Sure hey Chris.

00:02:58 Speaker 4

Hello Prasad, happy to be here to kick start this podcast series between and with HCL and several.

00:03:07 Speaker 4

So yeah, so it's Chris as he said.

00:03:09 Speaker 4

I'm Slava Bronfman and the CEO of Sabo I.

00:03:12 Speaker 4

I started actually my background and I started my professional career in the Israeli cyber Security Intelligence Corp.

00:03:18 Speaker 4

Leading cybersecurity products specially in the areas of IoT.

00:03:24 Speaker 4

And after discharging from from the army, from the idea if we founded Sabelo, couple of folks from from the army from the same unit and several military today helps automotive manufacturers to build and maintain secure connected components.

00:03:39 Speaker 4

And we do that using a very proprietary and unique technology.

00:03:43 Speaker 4

That's called.

00:03:44 Speaker 4

Cyber Digital twins where we where the system actually creates an identical replica of each automotive component which basically enables them performing vulnerability assessments and compliance validation on that on this digital artifact.

00:04:00 Speaker 4

And by then basically creating kind of a source of truth for product security help really manage the product security throughout the entire product lifecycle.

00:04:10 Speaker 4

It's me and excited about our conversation today and disperse adding increase.

00:04:18 Speaker 5

Yeah, thank you so hey Chris, I'm Prasad and helps the research division of HCL engineering and direct business as a team.

00:04:27 Speaker 5

We are responsible for technology research is in.

00:04:29 Speaker 5

The area of.

00:04:31 Speaker 5

Artificial intelligence computer vision robotics, extended reality blockchain and cybersecurity.

00:04:37 Speaker 5

And we are also responsible for open innovation, university relations and IP development along with partners like similar to address our customer needs.

00:04:45 Speaker 5

All of the.

00:04:46 Speaker 5

24 years in this industry have spent over seven years in leading teams for developing secure file systems, identity access management and the management products and that shell. That's what we do.

00:04:58 Speaker 3

Thank you Prasad.

00:05:01 Speaker 3

So gentlemen, I have to ask you, you know, will it?

00:05:05 Speaker 3

What is it that's bringing cyber security to the forefront and it's becoming such an area that many OEMs and many of the suppliers to the automotive industry are really starting to get more deeper.

00:05:21 Speaker 3

Into and starting to have this as part of their processes, and their focus is they're developing their products.

00:05:28 Speaker 1

What what, what's the?

00:05:30 Speaker 3

Catalyst in making this such an area of focus.

00:05:35 Speaker 4

So, so I think you have to really answer that question.

00:05:38 Speaker 4

We first need to understand really understand what's a vehicle today, right?

00:05:41 Speaker 4

The vehicle is not what he used to to know, you know, 20 years ago, which was a mechanical machine.

00:05:47 Speaker 4

It's more of a data center on Wheels, right?

00:05:51 Speaker 4

It's basically a device, and any device that is full of many small computers.

00:05:57 Speaker 4

It's called cues.

00:05:59 Speaker 4

And they are full of software today, really full of software and basically like you know, like any other component that is full of software, there are always cyber security risks to that right?

00:06:08 Speaker 1

Right?

00:06:12 Speaker 4

And also the vehicle today is right.

00:06:15 Speaker 4

This is very much connected, it has internal connectivity.

00:06:19 Speaker 4

Kind of an internal canvas network, but also external connectivity to the cloud of the OEM of the manufacturer, but also you know Bluetooth connectivity and Wi-Fi connectivity, and from an attacker point of view these are all attack vectors to the vehicle.

00:06:34 Speaker 4

So even small things, it is true that we still don't see today, right?

00:06:39 Speaker 4

Kind of terror attacks of vehicles being, you know, taking over taking over Rd, but we didn't do see many other things because of that lie because of all the software, software oriented, vehicle things like car sets, right?

00:06:54 Speaker 4

We don't.

00:06:55 Speaker 4

It's no longer like we used to, so in movies to see movies, uh, that.

00:07:00 Speaker 4

You know someone coming to steal vehicle and kind of wish there playing with the wires to steal that.

00:07:05 Speaker 4

Today you just need to hack the mobile app or the key file.

00:07:08 Speaker 4

The smart key FOB and voila, you can basically steal the vehicle and we see a trend of more and more vehicles being stalled out that way.

00:07:17 Speaker 4

But also there is today.

00:07:19 Speaker 4

You know, a lot of personal information.

00:07:21 Speaker 4

That is being stored stored in the vehicle and and as we see, you know personal information.

00:07:27 Speaker 4

Obviously there is also a financial kind of aspect to that where you're storing your credit card in the vehicle to pay.

00:07:35 Speaker 4

Or your, you know, electrical charge in the electrical charging station and basically you know similar to what we saw in the, you know, evolving in the IT world you know, same attacks like crossovers, right?

00:07:50 Speaker 4

Uhm, you know we expect to see them in in in the vehicles and pretty much the same way.

00:07:56 Speaker 4

Because again, it's an environment full of software.

00:07:59 Speaker 4

There is data there important data that is stored and with pretty much you know similar or or a bit of different attack vectors attackers might take control over this.

00:08:11 Speaker 4

Daytime eventually in future over the vehicle.

00:08:13 Speaker 4

So I guess you know all the connectivity and all the software things are really driving.

00:08:18 Speaker 4

You know the all the bugs that we here recently about the motive, cyber security and the great interest of OEMs and tier ones in in cyber security and ensure Prasad, you you see the same, you know from your side.

00:08:33 Speaker 4

With clients and so on.

00:08:35 Speaker 5

Yeah, absolutely so.

00:08:36 Speaker 5

So today's cards you know, if you look at right have up.

00:08:38 Speaker 5

To 100.

00:08:39 Speaker 5

And 50 issues and 100 million lines of code.

00:08:41 Speaker 5

That's what people say is and it is expected to be printed.

00:08:44 Speaker 5

Million lines of code in near future.

00:08:46 Speaker 5

So which means software.

00:08:47 Speaker 5

Electrical and electronic components and their extension to the back end system will continue to play an important role in driving this growth and innovation right in.

00:08:55 Speaker 5

The automotive industry.

00:08:56 Speaker 5

And you already touched upon some of the attack vectors like cellular, Wi-Fi, Bluetooth, calibration monitoring and is less keyless entry systems, right?

00:09:04 Speaker 5

But at the same time, we cannot ignore that attack vectors associated with the back end systems, right?

00:09:09 Speaker 5

So just to name a few, there could be login authentication entry points associated with the back end systems or admin interfaces.

00:09:16 Speaker 5

And the Kurian search functions, APIs, and interfaces to integrate with the third party systems.

00:09:21 Speaker 5

And most of these automotive cyber attacks can be divided into 2 categories.

00:09:25 Speaker 5

In my opinion, remote or physical attacks.

00:09:29 Speaker 5

And if you look into the remote attacks are in rice since 2010, accounting to 79.6% of all attacks in.

00:09:36 Speaker 5

The last 10 years.

00:09:38 Speaker 5

And that's an interesting data point that leads to another question in my mind why there has been a rise in cyber security attacks and what are some of the security vulnerabilities that a vehicle?

00:09:48 Speaker 5

Can be exposed to what's your take on that?

00:09:52 Speaker 4

Yeah, so so you know.

00:09:54 Speaker 4

Talking about vehicle vulnerabilities and abilities in general, again, it's very important to understand the automotive ecosystem and the automotive landscape, right?

00:10:04 Speaker 4

So what motive industry is a bit unique in in the way you know that it's kind of build upon supply chain right?

00:10:10 Speaker 4

And automotive OEM?

00:10:12 Speaker 4

Is basically one of you know there are basically integrate.

00:10:16 Speaker 4

Leaders are taking receiving gold.

00:10:19 Speaker 4

Most of the issues that are in the vehicle.

00:10:21 Speaker 4

Most of the software that is in the that is going into the vehicle from their suppliers from the Tier 1 suppliers but also in many cases are receiving a lot of debt from their Tier 2 suppliers and so on.

00:10:33 Speaker 4

And eventually you know they're assembling all these data receiving.

00:10:37 Speaker 4

All these black boxes and integrating that into into the vehicle so obviously supply chain attacks, supply chain risks and supply chain vulnerability.

00:10:45 Speaker 4

These are basically an integral part of that right?

00:10:49 Speaker 4

You really automotive manufacturers really need to make sure that their supply chain is secured at every ECU that there're or every piece of code.

00:10:59 Speaker 4

Or this software that they're receiving integrating into the vehicle is secured and you know free of.

00:11:05 Speaker 4

Backdoors, vulnerabilities, and basically build according to their, you know, cyber security requirements and.

00:11:13 Speaker 4

Practices and it is challenging right?

00:11:16 Speaker 4

Again in, especially in the environment of black box devices, right?

00:11:21 Speaker 4

You're receiving the completely black box device.

00:11:23 Speaker 4

Need to integrate it into the vehicle.

00:11:24 Speaker 4

It's challenging task and of course again because the vehicle is full of software so even you know regular thing that we are familiar with from.

00:11:34 Speaker 4

The environments.

00:11:36 Speaker 4

So software supply chain and open source software we see more and more open source software is getting into the vehicle, which is an obvious you know, trend because there there is a lot of software out there and reusing good software, open source software probably is the best practice for developing.

00:11:57 Speaker 4

So, but but it also comes with the risk.

00:12:00 Speaker 4

With that right in it.

00:12:01 Speaker 4

Like all the cities that we know, right?

00:12:04 Speaker 4

The open source related vulnerability is also commercial source commercial components and their vulnerabilities.

00:12:12 Speaker 4

We see a lot of them in the vehicle in the mountain of thousands of.

00:12:17 Speaker 4

Such open source related CVS in in single vehicle in single model that running on the roads today.

00:12:23 Speaker 4

And there is also also always the risk of you know zero day attacks and unknown vulnerabilities, especially for you know terror attacks in, you know, kind of high end malicious actors.

00:12:35 Speaker 4

And the last thing that I would like you know to to mention on that back to your question, Prasad is that it is.

00:12:43 Speaker 4

Challenging to update the.

00:12:46 Speaker 4

Software in the vehicle right?

00:12:48 Speaker 4

We see more and more over the rebels today, but there are still embedded microcontrollers.

00:12:54 Speaker 4

Usually you know autosar based components in the safety area of the vehicle that it is challenging to update them.

00:13:00 Speaker 4

So everything related to you know to outdated software and aging software which obviously pulled.

00:13:06 Speaker 4

You know, put their poses and an operational risk just by being you know, an outdated software, but also from a security perspective.

00:13:13 Speaker 4

It's really hard to patch it and keep it up to date, and you know with all the vulnerabilities patch.

00:13:20 Speaker 4

So you know pretty much see the entire spectrum of vulnerabilities, and you know spend specific vulnerabilities in in the automotive sector today.

00:13:32 Speaker 5

Interesting, so vulnerability is sustained with outdated components is one of the primary.

00:13:36 Speaker 5

Factors as well as.

00:13:37 Speaker 5

You said so, but along with that I can see insecure design is 1 aspect of it along with you know lack of perimeter security within the vehicle and as well as towards the back end services.

00:13:46 Speaker 5

Maybe the unencrypted traffic between you know the device and as well as the back end systems using that input traffic as a communication channel.

00:13:54

Right?

00:13:56 Speaker 5

And we also talked about exploring, you know, exploiting these in in vehicle vulnerabilities, right?

00:14:00 Speaker 5

One can gain access to towards infotainment navigation and telematics unit.

00:14:05 Speaker 5

And there's a back door to gain access to.

00:14:07 Speaker 5

The back end.

00:14:07 Speaker 5

Services as well, right?

00:14:09 Speaker 5

It's this, you know.

00:14:10 Speaker 5

Interesting point is exploiting.

00:14:12 Speaker 5

I was actually looking into that cycle.

00:14:13 Speaker 5

You know CV report and exploiting this back and one radius can lead to exposure of personal data and API keys as well right?

00:14:21 Speaker 5

And as well as token.

00:14:23 Speaker 5

And from there gain access to the in vehicle network or even launched more DOS attacks, right?

00:14:28 Speaker 5

And these normally falls under, you know, medium risk category.

00:14:33 Speaker 5

And then you actually talked about, like, uh?

00:14:37 Speaker 5

Uh, exploiting it up these in vehicle vulnerabilities as well, but don't you think this falls under low risk category and require an in depth knowledge of the connected car platform?

00:14:48 Speaker 5

What is your take on that?

00:14:50 Speaker 4

Yeah it is. It definitely requires you know in the app's understanding of the platform and of all the connectivity and so on.

00:14:58 Speaker 4

But you know, from from intermediate from an attacker POV and title, but you know, understanding how attacker thinks teaching me not.

00:15:09 Speaker 4

Challenge or not, the main challenge you know.

00:15:13 Speaker 4

This data eventually will be available.

00:15:16 Speaker 4

This knowledge eventually will be available, and it might take a bit more time.

00:15:20 Speaker 4

You know to to understand to learning to understand how the internals of the vehicles works and all protocols and all connectivity.

00:15:29 Speaker 4

But the you know from attackers, the good thing is that eventually they can buy one vehicle or find 1 architecture and there is a full fleet out of of the of the of those vehicles, usually running on the road.

00:15:42 Speaker 4

So you know the practice of protecting by just keeping things you know in secret usually fall short when you know we see attackers that really persistent and we like to act vehicles.

00:15:59 Speaker 5

And this one more rain at this point came to my mind and these back end services when we actually talked about, right?

00:16:05 Speaker 5

We actually talked about.

00:16:06 Speaker 5

High risk, low risk and high.

00:16:07 Speaker 5

Risk and medium risk and all.

00:16:09 Speaker 5

But these back end services are susceptible to traditional.

00:16:12 Speaker 5

Attacks like SQL injection cross site, you know, cross site scripting and sustain session hijacking.

00:16:17 Speaker 5

Particularly when they are.

00:16:19 Speaker 5

Getting hosted on Hyperscalers under shared responsibility model.

00:16:24 Speaker 5

And this also comes under other medium risk category in my opinion.

00:16:27 Speaker 5

Just you need to know how.

00:16:28 Speaker 5

To compromise traditional.

00:16:29 Speaker 5

You know multi layer ID defence systems and with a very limited knowledge of connected car internals, right?

00:16:35 Speaker 5

Do you agree with that?

00:16:37 Speaker 4

Yeah, absolutely.

00:16:38 Speaker 4

And by the way, it's great percentage.

00:16:39 Speaker 4

You're touching the and you know emphasizing all the back end systems.

00:16:43 Speaker 4

I definitely think that.

00:16:45 Speaker 4

Protecting vehicles it's not only thinking about the edge devices or the the vehicles themselves.

00:16:51 Speaker 4

It's the entire ecosystem.

00:16:52 Speaker 4

Eventually you you need to find, you know one access vector to to to have the entire ecosystem.

00:17:00 Speaker 4

The entire fleet or or or each you know particular vehicle just from the back end.

00:17:06 Speaker 4

So I do agree with you that it's you know like you said, it might be the weakest.

00:17:10 Speaker 4

You know the weakest link in your chain, so the back ends because eventually yeah, it is just traditional systems and traditional IT systems traditional ID server.

00:17:21 Speaker 4

So yeah, you're just you're raising your grade point.

00:17:26 Speaker 5

So it's clearly indicates that you know security does not stop at the production of vehicles, and security vulnerabilities can be discarded in the given time across ecosystem, right?

00:17:35 Speaker 5

And it will require Williams and supplies to detect and react to these security issues throughout the entire life cycle until the vehicle reaches its end of life.

00:17:44 Speaker 5

So that's my take on this course.

00:17:45 Speaker 5

I mean, in a nutshell, if you look into.

00:17:47 Speaker 5

The various aspects.

00:17:49 Speaker 5

Of cybersecurity, why it is becoming more prevalent nowadays and as well as what kind?

00:17:54 Speaker 5

Of vulnerabilities exist.

00:17:57 Speaker 3

No, it's it's very insightful and listening to both of you have that exchange.

00:18:01 Speaker 3

You know what came into my mind is.

00:18:04 Speaker 3

The vehicle is going to continue to evolve and get more and more complex technology in.

00:18:09 Speaker 3

It right we we.

00:18:10 Speaker 3

Talked about connectivity and over the air updates and five G's coming in.

00:18:14 Speaker 3

So there's gonna.

00:18:15 Speaker 3

Be more data transferred back and forth.

00:18:16 Speaker 3

To the vehicle.

00:18:18 Speaker 3

Higher amounts of.

00:18:19 Speaker 3

Electrification, which means we need to charge at public charging stations.

00:18:24 Speaker 3

Bringing in.

00:18:26 Speaker 3

Higher level of Autonomy's and ultimately someday full autonomous vehicles, you know, will be in the fleet and on the road.

00:18:33 Speaker 3

And with that.

00:18:34 Speaker 3

There's even a a change in the type of mobility people may want.

00:18:38 Speaker 3

We see some of it today with shared mobility, but that could even become more prevalent in the future.

00:18:44 Speaker 3

And as these changes.

00:18:46 Speaker 3

Develop in the future than that.

00:18:48 Speaker 3

How do you feel that the risk profile is going to change around cyber security and the need to make sure that there's you know higher protective levels around cyber security?

00:19:00 Speaker 4

I think it's a great question Chris, and our approach to that in Sebelum is always to understand that every new capability every new you know feature.

00:19:10 Speaker 4

Of course, all these capabilities are working on the way, but they are near actors.

00:19:17 Speaker 4

Actually, every new capability of the new technology.

00:19:20 Speaker 4

Basically, the code is especially those you know all those that we just mentioned.

00:19:26 Speaker 4

Her kind of software based and will have some software.

00:19:30 Speaker 4

Element in them.

00:19:31 Speaker 4

Not at that point into the vehicle so, and that's always how we think.

00:19:36 Speaker 4

So for example, you mentioned electrical vehicles, albeit replication vehicles are going through suggesting code where you know the charging station the new charging station, there, there, there, there is.

00:19:49 Speaker 4

You know there is some amount of data and fair amount of data that is going even transferred between the vehicle and the charging.

00:19:56 Speaker 4

Right from probably the credit card and other things about the vehicle itself, the the location of the vehicle.

00:20:05 Speaker 4

With some you know the game number to identify the vehicle itself, right?

00:20:10 Speaker 4

So now it's not only that you need to have the vehicle, you might just have the charging station and get all this data.

00:20:17 Speaker 4

And of course it's a new.

00:20:20 Speaker 4

It's kind of new communication with your protocol protocol that will be coming to protect.

00:20:26 Speaker 4

And the same goes for autonomous vehicles, right?

00:20:28 Speaker 4

So there are new talk vectors or tax scenarios that you know.

00:20:34 Speaker 4

I think security professional could never even think of like just think about, uh, attack that we just saw, I think last year that was shared by.

00:20:46 Speaker 4

Researchers from harm and we're saying demonstrated how, just like pretty and transparent kind of sticker on traffic assigning Rd sign that just change them completely, the meaning of their Rd sign, right?

00:21:02 Speaker 4

So in a problem.

00:21:03 Speaker 4

Vehicle sounds, camera capturing design might get a completely different.

00:21:10 Speaker 4

You know, meaning that so you can put some sticker that instead of a stop sign.

00:21:15 Speaker 4

Yeah, you can put their sound.

00:21:17 Speaker 4

You know limitation of your.

00:21:21 Speaker 4

Speed, speed, limitation and so on.

00:21:22 Speaker 4

So maybe you know for me Union high you cannot see that, but the vehicle can perform or understand that completely differently.

00:21:31 Speaker 4

And this is also even if it's not the traditional one.

00:21:34 Speaker 4

But this is of course a cyber attack.

00:21:37 Speaker 4

On the vehicle, right?

00:21:38 Speaker 4

It's eventually sensors.

00:21:39 Speaker 4

The software is understanding something.

00:21:41 Speaker 4

Try to to to act upon that sign and that you cannot.

00:21:47 Speaker 4

So yeah, just to summarize, of course, every new capability will introduce new person should.

00:21:56 Speaker 4

Per said you can.

00:21:58 Speaker 4

You probably have more and more examples to get from other use cases.

00:22:02 Speaker 5

Yeah, you covered.

00:22:03 Speaker 5

Uh, quite, you know, the kind of risk.

00:22:06 Speaker 5

That are, you know.

00:22:07 Speaker 5

These systems can get exposed to in terms of autonomous and decimals electrical vehicles.

00:22:13 Speaker 5

Let me touch upon shared mobility, right shared mobility as a trans certainly offers a potential growth and increase in vehicle utilization.

00:22:21 Speaker 5

There is no doubt about it.

00:22:23 Speaker 5

But these shared mobility platforms and applications could hold sensitive data.

00:22:27 Speaker 5

From hundreds of unique users, right?

00:22:28 Speaker 5

And presents the risk of sensitive data explosion, but also you touched upon is 1.

00:22:31 Speaker 5

Of the best right area.

00:22:34 Speaker 5

So it requires.

00:22:35 Speaker 5

Certainly a comprehensive approach to ensure full production of the user data right?

00:22:39 Speaker 5

I mean if I look into the last year I.

00:22:41 Speaker 5

Was seeing one of.

00:22:41 Speaker 5

The reports the hackers offered to sell car rental information of 3.5 million users of rental, a rental car company on the dark web, and such a breach of sensitive data could have an impact on the business model itself.

00:22:53 Speaker 5

And that's my take on the shared mobility.

00:22:55 Speaker 5

How this profile is going to change?

00:22:58 Speaker 5

And another dimension he also touched upon the mobile phones, right?

00:23:01 Speaker 5

Which isn't carrying devices like mobile phones or their digital cockpits with the same right?

00:23:07 Speaker 5

They're like phone on wheels, right?

00:23:08 Speaker 5

Like when phone with wheels.

00:23:10 Speaker 5

While these have made the user experience better, but they are becoming the primary attack vectors, right?

00:23:15 Speaker 5

Mobile apps or the third most frequently used attack vector?

00:23:19 Speaker 5

From 2010 to 2020, to access the vehicle and the back end services right.

00:23:24 Speaker 5

And so this is.

00:23:25 Speaker 5

Another interesting term that you coined.

00:23:27 Speaker 5

You know the cards are like there's a data.

00:23:29 Speaker 5

Center on Wheels right?

00:23:31 Speaker 5

And I completely agree with that.

00:23:33 Speaker 5

So in future connector cuts, could you know use the hybrid architectures to the way we.

00:23:37 Speaker 5

Use you know, I've read per.

00:23:39 Speaker 5

You know infrastructures in RIT world, like you know, safety and controlling functions can be left in the car itself, and the data and processor intensive use your functionalities can move to cloud and fisi, low latency, high availability network.

00:23:54 Speaker 5

And we to see connectivity.

00:23:55 Speaker 5

Modes can certainly make this possible, and this opens up another set of Pandora box of man in no man in the middle attacks or the DOS attacks.

00:24:04 Speaker 5

Silly naturally fail Mike categorize you know water under risk, right?

00:24:09 Speaker 5

So data collected, generated, stored and shared by the cars and by the back end systems.

00:24:16 Speaker 5

Physical access to the cars, including the driving services which we also talked about and network and processor resources of the cars and even energy resources of dielectric calls might be under risk as we move forward.

00:24:32 Speaker 3

That's a great point, Prasad.

00:24:35 Speaker 3

And I want to ask both of you when we look at the automotive industry as well.

00:24:40 Speaker 3

I mean, we, we know historically and even today automotive manufacturers are fiercely competitive.

00:24:48 Speaker 3

And the suppliers to those manufacturers are fiercely competitive.

00:24:53 Speaker 3

And there will be, you know, implementation of through, you know, working groups like an SAE or through regulations elements around cybersecurity that are going to be coming into play.

00:25:05 Speaker 3

But it's also, I think, quite interesting that around the topic of cyber security and given its importance to have a secure vehicle, we see some collaboration and maybe a way we haven't seen before in the industry and how have both.

00:25:23 Speaker 3

Have you seen that in your?

00:25:25 Speaker 3

Interaction with manufacturers or suppliers and discussions that you've had of how there is more collaboration around this topic of cyber security.

00:25:35 Speaker 3

And, you know, sharing of insights that traditionally as competitors might not have been shared.

00:25:44 Speaker 4

Yeah, it's a great point, Christina, and it's surprisingly, it's actually surprising what happened now in the industry.

00:25:51 Speaker 4

So as you said there, I think it's one of the most competitive area industries.

00:25:56 Speaker 4

The world right and very conservative 1 they're usually not sharing OEM sorted once, not sharing any information between them, even though.

00:26:05 Speaker 4

Again, they all share the same supply chain and probably using the same vendors for for everything they do, but.

00:26:14 Speaker 4

Again, as you.

00:26:15 Speaker 4

Said provisioning they are not sharing any information, but when it comes to cybersecurity, we apparently now see, I think something that is amazing that they are most of the empty ones.

00:26:26 Speaker 4

Or really, you know aiming for collaboration.

00:26:29 Speaker 4

And I think that's because they understand it's a necessity.

00:26:33 Speaker 4

You know, the pace of productivity in software in the vehicle is a lot, you know faster than they are able to protect the vehicles or propanol.

00:26:42 Speaker 4

This is that phase, so we see them collaborating in, you know, in Isaacs, like in the optimizer where we see you know.

00:26:50 Speaker 4

Create a lot of volume Cynthia wants participating in sharing information.

00:26:55 Speaker 4

I think also the the slogan of applies the keys and the things they're saying.

00:27:00 Speaker 4

Then attack on one is an attack on all.

00:27:02 Speaker 4

Which is basically not emphasize what it's going. Well, kind of soft process of OEM's not today in the industry and the same thing we're seeing, you know, in moderation instead rotation.

00:27:16 Speaker 4

So we say when we participated, for example in the in the ISO 21434 were part.

00:27:22 Speaker 4

With the drafting committee, and we saw that pretty much all the yams and key ones across the globe kind of got together as part of the ISO.

00:27:32 Speaker 4

Or they see and participated together to.

00:27:36

You know to.

00:27:37 Speaker 4

Build the best cyber security standard in cyber security engineering standard.

00:27:42 Speaker 4

Actually the first one, four or four vehicles and there were, you know, sharing information about what are the best practices, how they view that and eventually it took awhile.

00:27:52 Speaker 4

A couple of years that eventually this year was released.

00:27:56 Speaker 4

The final.

00:27:57 Speaker 4

Version of the first version of the standard, and we see that I'll actually be in the doctor, but by all players really across the board.

00:28:06 Speaker 4

And we think the same with, you know with the new WP 29 Regulation, the European one that is also being deducted in many areas in the world.

00:28:16 Speaker 4

Come, yeah, so you know we see it's a great deal of that not get that good in the adoption side, right?

00:28:23 Speaker 4

So they are collaborating.

00:28:24 Speaker 4

There is a huge collaboration but still not that enough adoption.

00:28:30 Speaker 4

No, but just the recent survey of civilians so that less than about 30% of our players of William City once haven't even began to compliance and just about 65% are just in the middle preparation, which which means that had just a very small percentage of programs that are.

00:28:50 Speaker 4

Meeting already those all those regulations and compliance.

00:28:54 Speaker 4

Come here in terms of collaboration save greatly, you know, cross OEMs across regions.

00:29:01 Speaker 4

They're collaborating, which is great ideas for the industry.

00:29:07 Speaker 4

These in the market.

00:29:09 Speaker 5

Yeah, I mean it's the.

00:29:10 Speaker 5

Same thing that I'm I'm also observing, and if you look at the current Trent Williams are building their own cybersecurity components, or even.

00:29:17 Speaker 5

Software stacks right?

00:29:19 Speaker 5

And suppliers are offering special cyber security consulting services vertically along the value chain, both up.

00:29:24 Speaker 5

And down right?

00:29:26 Speaker 5

And startups, I don't have to.

00:29:27 Speaker 5

Say much here in on that and.

00:29:29 Speaker 5

Entering into the market with innovative.

00:29:30 Speaker 5

Solutions like you know.

00:29:33 Speaker 5

And even interesting aspect is cyber traditional cyber security product companies are expanding into the automotive cybersecurity market as an adjacent market space, right?

00:29:41 Speaker 5

This is 1 dimension to it.

00:29:43 Speaker 5

And then you also talked about, you know OEM sources, large share of their components from suppliers in semiconductor manufacturers so.

00:29:51 Speaker 5

Internet shell in all.

00:29:52 Speaker 5

Participants in the valuation need to follow and implement cyber security practices to mitigate these risks, right?

00:29:57 Speaker 5

Even though volumes are ultimately responsible for the cyber security and no security team can keep up with the average number of new vulnerabilities posted each day, right?

00:30:07 Speaker 5

And they won't be able to cover all.

00:30:08 Speaker 5

The ones that are already out.

00:30:09 Speaker 5

There, and certainly this presents an opportunity to collaborate by sharing insights and from the recent attacks and as well as joining forces to fight.

00:30:17 Speaker 5

The future ones.

00:30:18 Speaker 5

And these could be as a, you know, in the form of joint cyber security research and certification or a joint VSAT services between all participants.

00:30:26 Speaker 5

Right?

00:30:26 Speaker 5

This is 1 dimension second aspect you talked about.

00:30:30 Speaker 5

And coming in in terms of WP 29 and I.

00:30:32 Speaker 5

I said to 1434.

00:30:34 Speaker 5

But coming up coming into that, you know upcoming policies and regulations on cyber security.

00:30:40 Speaker 5

Certainly, in my opinion they will allow the automotive industry to implement common cyber security practices throughout the vehicle lifecycle, right from vehicle development through production and all the way to post production, right?

00:30:53 Speaker 5

But are we?

00:30:54 Speaker 5

There yet, in my opinion, it is not. I mean, you actually refer to your survey, and I'm also referring to the same server right? Only 6% of the participants are fully prepared for these regulated requirements. As for the subway.

00:31:05 Speaker 3

Yeah, I agree with the points that both of you have made in Slav.

00:31:08 Speaker 3

As you just said.

00:31:09 Speaker 3

I mean, this is a whole topic that can be discussed in it of itself in quite some depth and detail.

00:31:16 Speaker 3

And at our next podcast we're actually going to take time to do that.

00:31:20 Speaker 3

Spend a little bit more, and go into a deeper dive on on how policies.

00:31:25 Speaker 3

Or changing what regulations are coming on the element of collaboration amongst the industry, training and retraining of people, and so we'll spend more time on that in our next podcast.

00:31:37 Speaker 3

But we're out of time for today, so Prasad and Slova.

00:31:41 Speaker 3

I want to thank you for joining us today and sharing your insights.

00:31:45 Speaker 3

Oslava for helping us to look at a vehicle as a data center on wheels. I think that's a big take away for us from this and Prasad for reminding us that we can't forget about the back end.

00:31:57 Speaker 3

We can't think only about the vehicle but where it's connected to and all the back end services so.

00:32:03 Speaker 3

Come to our audience, I would like you to invite you to join our next.

00:32:09 Speaker 3

We will have two other industry experts joining us to delve deeper into cyber policies, pending regulations and the impact it will have on automotive development, testing, validation and monitoring.

00:32:24 Speaker 3

Thank you for joining us today.

00:32:28

Thank you.