00:00:01  
*Speaker 1:* So can you please introduce yourself a little bit?

00:00:05  
*Speaker 2:* So my name is Michael Carbone. Uh, I'm an associate professor here. I'd like to you. I've been here since, uh, 2009, actually. So I was a very long time. And, um, my research area is, uh, uh, software verification. Uh, and I mostly work with theoretical in, uh, in the theoretical computer science area. I'm also a member of the CSat center, which is our center for information. Uh, trust. Uh, no. Sorry. Information security and trust. And, um, I am, uh, also had in the, uh, our master's in computer science, as I do.

00:00:56  
*Speaker 1:* Great.

00:00:56  
*Speaker 2:* Is that enough?

00:00:57  
*Speaker 1:* Yeah. So How do the session types and the choreography contribute to ensuring the correctness and security in web service interactions?

00:01:11  
*Speaker 2:* Yeah. So, um, so the idea is that, uh, so basically these choreographies and session types are um, uh, languages for specifying, uh, protocols. Uh, so communication protocols. So you have these, uh, I mean, web services, uh, is an application of that. Uh, but it's not necessarily web services, but any communicating, uh, entities, uh, in a distributed system, they interact with each other and they all run code and exchange information. And what you want to use, what you want to do is to use what you can do. Sorry, is to use these, uh, choreographic, uh, protocol languages for specifying how they have to exchange information. And then what you can do is to use this specification and design some tools that can check that the code is actually faithful and to, to to those specifications. So it's not really security, but it's more like a more general concept, which is correctness. Uh, and security is basically one particular, uh, aspect of that.

00:02:26  
*Speaker 1:* So what are the fundamental trade offs between the expressivity and security in languages for concurrency?

00:02:37  
*Speaker 2:* What was the first thing you said? Sorry.

00:02:39  
*Speaker 1:* The expressivity.

00:02:41  
*Speaker 2:* Uh, expressivity. And what's the other? Say it again. Can you say it again? Completely say it again.

00:02:47  
*Speaker 1:* What is the fundamental trade offs between the expressivity and security in the languages for concurrency?

00:02:56  
*Speaker 2:* Um, so usually what you want to do there is that, um. Uh, you want to, to these languages that basically specify how entities in the system have to, to, to exchange information. Um, they can be very simple. Uh, and they can also be very complicated. So the more, um, the simpler they are, the easier it is to actually verify that your software is actually compliant, let's say, to these specifications. Um, uh, but of course, uh, the simpler it is, the less expressive it is. So you so, you know, when, if you, uh, if you want to think, do things very easily, then of course, you lose, uh, a lot of expressivity. So you cannot specify basically some uh, uh, guarantees a, some, uh, correctness. But I mean, it's like security actually is a really good example of that. I mean, how much do you want to make your system secure? Right? And, uh, depending on how, uh, expressive your, uh, your tools, uh, your languages for specifying these properties are, uh, depending on how they are, then you can guarantee different levels of security, right? So it's, uh, which means that it's completely hard to say. Oh, this thing is perfectly it's perfectly security in most cases, at least. Uh, although you can we can start saying, oh, this thing is sort of secure on this particular aspect. This is actually very nice because at this point you can start talking about, uh, even probabilities, right? And then starts this is actually one of the stuff that I work on, which is like, okay, how secure is the system? Then you no longer say it's secure or secure is not secure. You just say, oh, 90% of the case is going to be fine.

00:05:05  
*Speaker 1:* So how how can static analysis techniques be applied to detect and prevent security vulnerabilities in concurrent and distributed systems?

00:05:16  
*Speaker 2:* Oh, well, there is, uh, there are decades of research on this. And, um, what I mostly interested in is actually, yes, you apply static analysis, which is the idea is that you want to, uh, it's what I was telling you in the beginning. You want to just, uh, uh, have some, uh, some code and then ask yourself, is this code secure? Is this code correct? And what you do is that you you basically use static analysis, which is like it's basically a tool that is going to inspect automatically, uh, your code, and it's going to give you an answer there with, uh, is it secure? It's not secure How secure is it? How correct is it?

00:06:01  
*Speaker 1:* So what are the biggest challenges in verifying the security properties in large scale concurrent systems?

00:06:11  
*Speaker 2:* Uh, the biggest challenges are that, uh, it's complexity. So, uh, uh, nowadays, these, uh, systems, uh, I mean, all all systems or all IT systems are distributed. So, uh, not only, you know, we are into into different locations and we are communicating with each other and we are exchanging information, but also in just inside your laptop, there is, uh, everything is also this concurrent distributed in there. And the point is that, uh, uh, as we advance technology advances, these systems become more and more complex, uh, which means it becomes harder and harder to actually program them. So, yeah.

00:06:56  
*Speaker 1:* How can trust based systems be effectively integrated into the web service architectures to enhance security and reliability?

00:07:09  
*Speaker 2:* Um, well, the the again, this is uh, it is not really what I'm doing uh, anymore at least. But uh, yeah, that there are there is a lot of research on this on uh, how to, to, to to develop and implement these trust based systems. But uh, uh, they are integrated by developing tools and techniques for, uh, for, for, uh, dealing with them. So, uh, sorry, maybe this is not a, uh, a complete answer, but, uh, it's, uh, it's part of the development of these systems. Yeah.

00:07:51  
*Speaker 1:* So what are the security implications of emerging technologies like AI driven optimization in web services and cybersecurity.

00:08:03  
*Speaker 2:* That's a good question. So you said AI, right? Yeah. And by AI you mean uh, uh, what we nowadays they call AI, these, uh, autonomous things that they try to, to do something by themselves. Um, but because I as a, as a much broader term, I think so it's difficult to, uh, but. Yes, um, uh, I mean, it can be integrated, but, uh, uh, how I mean, we we will find out. Uh, I think people are abusing nowadays there's, uh, AI tools and, uh, I think they can. Instead of using them to design the systems. Because that's a that's a bad idea. I think unless where they, they are further developed. But with the current state of the art, I don't think that's a good idea. But on the other hand. And that's where they are really successful. Successful already they can be used to find, uh, bugs and these kind of things because then they can inspect, uh, code or systems in general, interact with them and try to find out in a more efficient way actually, than traditional methods. They can find out whether there are bugs or discovered or security, uh, issues in this kind of thing.

00:09:25  
*Speaker 1:* So what are the major cyber security risks associated with the increasing digitalization of critical infrastructures?

00:09:38  
*Speaker 2:* Oh, that's a good question. Um, I don't know. Uh, there are many security threats. Uh, I would say that, uh, that, uh, I mean, the nowadays the most, the most, uh, uh, reliable thing that we, I mean, the most precious thing that we all have is data and, uh, how this data is handled and, uh, how it's going to be used, uh, also in the future. And what, um, uh, control we have over it. I think that's the, the, the, the hardest thing that we can, uh, that we need to solve because, uh, you know, there are all these regulations like GDPR, for example, in the EU. That's very, a very, a very interesting thing. But going from there to, uh, being able to have full control over your data or your whatever you can is yours and whatever is not yours. I think that that's, uh, we are far from that solving this problem. Yeah.

00:10:51  
*Speaker 1:* How do regulatory frameworks impact the security and privacy of distributed and cloud based web services.

00:11:03  
*Speaker 2:* Yeah, this goes back. I mean, regulatory framework like GDPR, I guess. You mean that kind of stuff. Uh, I mean, it's a it's a positive impact from, uh, a security perspective. Uh, but then, of course, as a price, you have to pay, right? Uh, that, uh, you know, uh, everything you do, uh, has to go through these extra checks and these extra, uh, protocols or processes that, uh, make things harder. I mean, it's like when you everytime you see a web page that to a new web page, you need to say yes or no to cookies, and, uh, eventually. That's really annoying, right? And, uh, uh, if there was not these regulations, we wouldn't have that, but then we would pay with something else. So it's always finding out, uh, what the trade off between, uh, what you want to guarantee and what you want to pay for. Uh uh, but they are impacting also I mean, from, uh, performance point of view, efficiency and these kind of things because they, of course, they add some overhead to anything where they need to be used.

00:12:13  
*Speaker 1:* So what role do decentralized technologies such as blockchain play in enhancing trust and security in global digital ecosystems?

00:12:28  
*Speaker 2:* Uh, it's um, probably they are uh, uh, they have some advantages. Uh, and uh uh uh, I mean, like blockchain, for example, they are not centralized. Therefore you don't need to trust anyone. You just trust, uh, uh, well, if you are an expert and you understand how these, uh, technology, decentralized technologies work, then, uh, yeah, you can stop trusting you just understand how they work. And then you actually, you can stop trusting how someone else who is, uh, otherwise you should rely on, like, centralized things. It's that, uh, the problem is that, uh, the, uh, the average person, uh, doesn't understand the technology. And then the question is, okay, you're moving your trust from, uh, one centralized entities, that being, I don't know, even the government or whatever or company or whatever to, uh, trust in the technology. And there of course, we don't know if you don't understand it, and you need to believe you have trust in others, but, uh, yeah, that's, uh, there's still a you need to trust something, uh, if you don't understand it. So I would say most people don't. So. Yeah. Please.

00:14:00  
*Speaker 1:* So what is the main threat in nowadays? For technology, the cyber threat?

00:14:10  
*Speaker 2:* Uh, for technology. What do you mean?

00:14:14  
*Speaker 1:* So what is the biggest threat for people right now, like from cyber warfare?

00:14:22  
*Speaker 2:* Oh, like, um. Uh, well, I mean, as a technical person, I would go back to data to what I said before, but, uh, uh, the impact of that, maybe it's even, uh, it's even worse because people who control data and control your data and you're not aware of them can also have an impact of you. So it can have a much a bigger, big and much bigger impact. Uh, in, uh, in society because it can influence what people think and what we've seen. There's already quite a lot in the last few, many years. So I would say this is the biggest threat. Uh, uh, but yeah, there's, um, there's other smaller threat that we care about, maybe as, uh, people who work with technology. But, uh, I think there is much more on top of that that would affect the whole society, not only, uh.

00:15:27  
*Speaker 1:* As how does, uh, cyber attack on the health institution can possess danger for the society.

00:15:37  
*Speaker 2:* On the on the what? Sorry.

00:15:38  
*Speaker 1:* Healthcare institution.

00:15:41  
*Speaker 2:* Healthcare.

00:15:42  
*Speaker 1:* Yeah.

00:15:43  
*Speaker 2:* Uh oh. Uh, so let me make sure I understood. So how does, uh, uh, Cyber attacks to the health care system. Could, uh, could could are dangerous for society. Uh, assuming that nobody wants to harm anyone, which is not the case, but maybe that's the. That would be an obvious, uh, consequence. But, I mean, if you can access the I mean, the whole health care system here in Denmark now is really strongly dependent on, uh, on it dependent. And which is good. It makes things efficient, makes things cheaper. Uh, and it allows, uh uh uh, it allows us to actually provide health care to more, even more people quicker. So this is a really good thing. Uh, again, the the issue is, uh, how this information is, uh, is handled and where it's kept and, uh, you know, uh, it could be that, uh, maybe in ten years we find out that, uh, our health system here, its sharing our information, our ways. I don't know, insurance companies, for example, or, uh, uh, some other company that could take advantage of this information and keep different policies, uh, you know, uh, different, um, uh, fees charge people differently because of, of this information, right. If they find out that I have a heart problem, then most likely they will pay that off. And, um, and again, this is this goes again into data. Where is this data stored? How much control do we have over this data and how the the state in this case can central I can, um, guarantee that this data is actually used in uh, in the right way. And we don't know how the, I mean, the, uh, average citizen, I have no idea how they are handling this because I don't even understand what it means to understand it.

00:17:58  
*Speaker 1:* How does geopolitical competition shape the development and adoption of secure digital infrastructures?

00:18:11  
*Speaker 2:* Well, um. I would say that in the last few years, uh, things a little bit, uh, have been a little bit more clear. Um, so clearly at the moment, I mean, uh, especially in, uh, if you work for, uh, for, uh, public institution also in private institutions, there is a lot of control on, uh, uh, how you can, uh, you can uh, uh, develop, uh, technologies in general, let's say it itself, uh, and who, uh, whom you can collaborate with. Uh, so I would say that now the situation is like you cannot work with Russian, so you cannot work with Chinese. Uh, full stop. There's not no discussion on that. Um, so, yes, it has an impact. And, uh, I can see that nowadays there is there are many more incentives on developing, uh, technologies. Uh, and, uh, um, how do you call it in, uh, in defense rather than investing, I don't know, into healthcare maybe, or these kinds of things. So, yes, uh, there is much influence because, uh, here I would go to research, which is what I, what I do, uh, I can see that there is more funds in these kind of things than other things that I would like to do. For example, uh, and uh, since there is more funding in those areas. That's where people start switching to, because that's the only way you can get some money to to do more research. So so there is an impact, I would say. And uh, uh, and this shifts all the time, right? I mean, now it's like, yeah, it's the problem is Russia is Ukraine and Italy is of course, but and China. But maybe ten years ago it was something else. And uh, I remember when I joined ITU in 2009, we were best friends with China and we had a lot of exchange problems with China. Now this is forbidden completely. So and of course, we were you were working on certain things by collaborating with some Chinese universities. Now we have we cannot do that anymore. And we need to work on different things or it is really a redirect. It actually works. Researchers do in general, not only cyber security.

00:20:47  
*Speaker 1:* So how do you see the future of Denmark's digital infrastructure evolving, and what cybersecurity measures should be prioritized to mitigate emerging threats.

00:21:01  
*Speaker 2:* Uh, well, unfortunately, they don't completely coincide. Uh, what I what I see is that, uh, I think at least as far as cyber security is, is, uh, is concerned, uh, unless, uh, the world, uh, changes, uh, it might be the case. Uh, you know, it's very dynamic. I can see Denmark going stronger and stronger into defense and, uh, investing a lot in that. Uh, what I think instead is that we should more, uh, develop, um, uh, the, I mean, the cyber security aspect of our I.T infrastructure, uh, not because of war, but because of, uh, we want to, to to make sure that our citizens are safe also within Denmark, without looking at threats from the from from the outside. So investing more in what you were mentioning like healthcare as well, or, you know, financial systems and these kind of things, are they secure enough? No, they are not elections voting. I mean, we have, uh, these kind of things. We clearly know that, uh, they are not perfect systems. And we should invest more in these kind of things for, you know, for a better democracy, actually, rather than investing more in water. But, yeah, there are also other threats that we need to worry about too. So I'm not saying that, uh, whoever is deciding is wrong, but, uh, it's, um, unfortunately, it's not as it should be. Yeah.

00:22:45  
*Speaker 1:* Yeah.

00:22:47  
*Speaker 2:* Yeah, I don't have any more questions.

00:22:49  
*Speaker 1:* Um.

00:22:50  
*Speaker 2:* So.