Interviewer: So can you please introduce yourself a little bit?

Researcher: I'm an associate professor here at “University A”. I've been here since 2009, actually, so a very long time. My research area is software verification, and I mostly work in the theoretical computer science area. I'm also a member of the CSat center, which is our Center for Information Security and Trust, and I am the head of our master's in computer science program.

Interviewer: How do session types and choreography contribute to ensuring the correctness and security in web service interactions?

Researcher: The idea is that choreographies and session types are languages for specifying communication protocols. Web services are an application of that, but it's not necessarily limited to web services - it applies to any communicating entities in a distributed system that interact with each other, run code, and exchange information.

What you can do is use these choreographic protocol languages for specifying how they should exchange information. Then you can use this specification to design tools that check whether the code is actually faithful to those specifications. It's not really just about security, but a more general concept of correctness, with security being one particular aspect of that.

Interviewer: What are the fundamental trade-offs between expressivity and security in languages for concurrency?

Researcher: These languages that specify how entities exchange information can be very simple or very complicated. The simpler they are, the easier it is to verify that your software complies with the specifications. But of course, the simpler it is, the less expressive it is, so you lose the ability to specify certain guarantees or correctness properties.

Security is actually a good example of this trade-off. How secure do you want to make your system? Depending on how expressive your languages are for specifying properties, you can guarantee different levels of security. It's hard to say something is perfectly secure in most cases, although you can say it's secure in particular aspects. This is where you can start talking about probabilities - which is one area I work on. Instead of saying a system is secure or not secure, you can say it's secure in 90% of cases.

Interviewer: How can static analysis techniques be applied to detect and prevent security vulnerabilities in concurrent and distributed systems?

Researcher: There are decades of research on this. With static analysis, the idea is that you want to examine some code and ask, "Is this code secure? Is this code correct?" Static analysis tools automatically inspect your code and give you an answer about how secure or correct it is.

Interviewer: What are the biggest challenges in verifying security properties in large-scale concurrent systems?

Researcher: The biggest challenge is complexity. Nowadays, all IT systems are distributed. Not only are we in different locations communicating and exchanging information, but even inside your laptop, everything is concurrent and distributed. As technology advances, these systems become more and more complex, which means it becomes harder and harder to program them correctly.

Interviewer: How can trust-based systems be effectively integrated into web service architectures to enhance security and reliability?

Researcher: This isn't really what I'm doing anymore, but there is a lot of research on how to develop and implement these trust-based systems. They are integrated by developing tools and techniques for dealing with them as part of the development process.

Interviewer: What are the security implications of emerging technologies like AI-driven optimization in web services and cybersecurity?

Researcher: That's a good question. By AI, you mean these autonomous systems that try to do something by themselves. I think people are currently abusing these AI tools. Instead of using them to design systems, which I think is a bad idea with the current state of the art, they can be very successful at finding bugs. They can inspect code or systems, interact with them, and try to find bugs or security issues more efficiently than traditional methods.

Interviewer: What are the major cybersecurity risks associated with the increasing digitalization of critical infrastructures?

Researcher: There are many security threats. I would say that nowadays the most precious thing we all have is data - how this data is handled, how it's going to be used in the future, and what control we have over it. That's the hardest problem we need to solve. There are regulations like GDPR in the EU, which is very interesting, but we're far from solving the problem of having full control over what's yours and what's not yours.

Interviewer: How do regulatory frameworks impact the security and privacy of distributed and cloud-based web services?

Researcher: Regulatory frameworks like GDPR have a positive impact from a security perspective. But there's a price to pay - everything you do has to go through extra checks and processes that make things harder. It's like when you visit a new webpage and need to say yes or no to cookies - that's really annoying, but without these regulations, we would pay in other ways. It's always about finding the trade-off between what you want to guarantee and what you're willing to pay for. These regulations also impact performance and efficiency because they add overhead.

Interviewer: What role do decentralized technologies such as blockchain play in enhancing trust and security in global digital ecosystems?

Researcher: Decentralized technologies like blockchain have some advantages. They're not centralized, so you don't need to trust anyone - you just trust the technology. If you're an expert and understand how these decentralized technologies work, then you don't need to rely on centralized entities. The problem is that the average person doesn't understand the technology. You're moving your trust from centralized entities like governments or companies to trusting the technology itself. If you don't understand it, you still need to trust something or someone, and most people don't understand blockchain technology.

Interviewer: What is the biggest threat for people right now from cyber warfare?

Researcher: As a technical person, I would go back to data. People who control your data and whom you're not aware of can have a major impact on you. They can influence what people think, as we've seen quite a lot in recent years. I think this is the biggest threat - one that affects the whole society.

Interviewer: How does a cyber attack on healthcare institutions pose danger for society?

Researcher: The healthcare system in Denmark is now strongly dependent on IT, which is good - it makes things efficient, cheaper, and allows us to provide healthcare to more people more quickly. The issue is how this information is handled and where it's kept. It could be that in ten years, we find out that our health system is sharing our information with insurance companies or other entities that could take advantage of this information - charging people differently based on their health conditions, for example. Again, this comes back to data: where is it stored, how much control do we have over it, and how can the state guarantee this data is used appropriately? The average citizen has no idea how this data is being handled.

Interviewer: How does geopolitical competition shape the development and adoption of secure digital infrastructures?

Researcher: In recent years, things have become clearer. If you work for public or private institutions, there's a lot of control over how you can develop technologies and who you can collaborate with. Currently, you cannot work with Russians or Chinese, full stop. There are now many more incentives for developing defense technologies rather than investing in healthcare or other areas.

In research, which is what I do, I see more funding in defense-related areas, which shifts where people focus their work since that's where the money is. When I joined “University A” in 2009, we were "best friends" with China and had many exchange programs. Now, this is completely forbidden. We cannot collaborate with Chinese universities anymore, so we need to work on different things or redirect our research.

Interviewer: How do you see the future of Denmark's digital infrastructure evolving, and what cybersecurity measures should be prioritized to mitigate emerging threats?

Researcher: Unfortunately, what I see and what I think should happen don't completely coincide. Unless the world changes, I can see Denmark investing more and more in defense.

What I think instead is that we should develop the cybersecurity aspect of our IT infrastructure not because of war, but to ensure our citizens are safe within Denmark. We should invest more in securing healthcare, financial systems, elections, and voting - these systems are not perfect, and we should invest more in them for a better democracy rather than investing more in war. But there are also other threats we need to worry about, so I'm not saying the decision-makers are wrong, but the situation is not as it should be.