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

00:00:07  
*Speaker 2:* My name is Dan. I'm a professor at IU and my research is in machine learning, and particularly within what I call AI information. So the stuff information that we can measure and obtain from mostly human eyes. Um, yeah. So that's what I've been doing for, for many years in developing AI trackers and methods for analyzing the data, inferring stuff about humans from, from mostly from mice. But I also do other things. So yeah.

00:00:44  
*Speaker 1:* Oh, I got great. So how do I based biometrics compared to traditional methods like fingerprints or facial recognition in terms of security and resistance to spoofing?

00:01:00  
*Speaker 2:* Oh, that's I think that's some very significant and very important differences. Um, so, so you can identify a human being from multiple factors and much more than people actually think. So Iris recognition is a very well known. But if I told you that the way that you move your eyes, the way that when you're exposed to certain things, also reveal who you are and you can't control it by any means. So with facial recognition or face recognition, with fingerprints, you can alter, but you can't do that with the with things happening in your brain that is reflected in the way you move eyes. So I think that that makes a a profound difference in, in, um, in the amount of information you actually gain and with the reliability of some of it, iris recognition is very well known and it scales very well. So that that is well known. I think what people don't know very often is this thing with the eye movements, that they actually really reveal a lot about you. What are your interests, what are who you are, what you're doing, what are your various aspects of cognition? Um, and you made and since you don't know it, you don't know what you give consent to when you when you do this. So, so I think it makes a difference. Mm.

00:02:36  
*Speaker 1:* Can gaze patterns be used for continuous identification. And how does this improve the security over one time authentication methods.

00:02:46  
*Speaker 2:* Yes. So yes the answer is yes. It has been done. Um, I mean how well it compares to other things. That's another matter. But it can be used for identification. Uh, it can also be used for entering passwords like like passwords. So all of this. Yes it's possible. So yeah. So you can say that if you look at the iris pattern that defines essentially that defines who you are. So the name and then you can have your gaze patterns reveal the password for example that has been that has been done. Um and some passwords are more believable than others. Wow. So if you write your own name. Julia, where are you from, by the way? I'm sorry.

00:03:41  
*Speaker 1:* Oh, I'm from Ukraine.

00:03:42  
*Speaker 2:* Are you all from Ukraine? Okay. I was, I thought, but, uh, due to the. Your first name. But I was confused by your last name. So why are you doing research at HQ or, uh.

00:03:56  
*Speaker 1:* I'm writing my bachelor thesis right now. Oh.

00:03:59  
*Speaker 2:* Okay. Okay. Okay. Okay. Um. Okay. So. So yes, there are some. So you can, you can get both passwords and identity, uh, as part of the information from the eyes. Yes.

00:04:18  
*Speaker 1:* How do you address the potential attacks, such as reply attacks of deepfake based spoofing on gaze tracking authentication systems?

00:04:29  
*Speaker 2:* We don't. Uh. Um, no, it's an interesting question. Um, I haven't seen many people do. I mean, generative models on AI. I mean, you can do it to some degree, but what is not known and why I'm a little bit reluctant to say something clever about this is that you can say that there's a you can all our information that's my claim, is governed by a sort of a triangle. Uh, and please don't publish this. But I'll tell you now I'm writing something about it at the moment. So, um, so you can say that it's. It's a triangle of who you are, what you're doing, and where are you doing it. So that is what governs these groups of parameters. Govern what, uh, your eye movements. But then but not all parameters might be present for all kind of tasks, for all persons, for all contexts. So. So for example, when you are driving a car, your eye movements might look something, uh, in one way, but that might also resemble other tasks where you are riding your bike or you're running or something else. So so there's an overlap. And that's why I'm saying I'm a little bit reluctant to say that you could do something with these spoof attacks. Uh, you can spoof iris recognition or Iris patents. That's that has been done. It's not it's not impossible at all. The question is, do they resemble the ones that you already have seen in your database? Um, and if you already know this pattern. Yes, that that is uh, then then you also know the name of the person, right? Um, and you can always when you know the person's name, you can enter that one chooses. So, so that is sort of one way. But then most authentication systems have a set of other parameters that they use, for example heat to uh do they see heat around in the face. So if you just have a screen that generates a pattern, it will not generate the right, uh, pattern. So then um, are the eye movements. Do they move in their natural way? Whatever you however you define this, um, and all sorts of things that they do to, to prevent you, that's not my specialty, but, uh, I know a little bit of it. Uh, but in general, of course, when you work with generative models, if they are true underlying and modeling the underlying distribution, you're sorry. Don't quote me on this. You're fucked. Uh, because, uh. What? How can you a system distinguish these things here unless you have some some other parameters? Yeah.

00:07:21  
*Speaker 1:* Hmm. Where does it make sense? Yeah. Are there any known adverse adversarial attacks that can trick eye tracking based on biometric systems? If so, how can they be mitigated?

00:07:38  
*Speaker 2:* Try to say this again. How are there any. What?

00:07:43  
*Speaker 1:* Are there any known adversarial attacks that can trick eye tracking based biometric systems? If so, how can they be mitigated?

00:07:54  
*Speaker 2:* Generative model. So so as I just pointed out, if you generate an iris pattern and it looks sensible, like, uh, Julius, uh, eyes. Well, you can try to log into the system, right? Uh, and if you can also generate live sequences with heat, uh, with the movements with all sort of that circumvented. That's. Well, like Carson Sherman says, there's no digital system that's safe. And this is an example of it, I think.

00:08:30  
*Speaker 1:* Since games can reveal personal and psychological traits, what are the main privacy risks associated with continuous eye tracking?

00:08:45  
*Speaker 2:* Main risks. Yeah. Many uh, I think that I mean, I think the biggest risk right now is that we don't understand the AI as a signal, period. Uh, so we don't we cannot assess the real risk. Uh, we don't know when you move your eyes. Is it Julia? Well, sometimes you can distinguish people, but. I. And you can also reveal some traits about your efficiency in reading. What is you pay attention to. But you are not. Never 100% sure, because you have a full set of different possibility interpretations of the same things. But that doesn't mean that you're not given extra information. So just like the governor's example, that, okay, if you have some information and you combine it with something else, um, you suddenly know much more. So the problem is that you're getting more than one bit of information. And when you have one bit of information, you gain something. And that means that you can also remove other things. So so when companies like meta and other, they actually want to have your AI data. They do this at the moment in the virtual reality and extended reality headsets. You are giving them a lot of information, and they join these with all sorts of other data that they have that they are profiling. So what they get now is that a much finer, detailed information about individuals. And are you aware of this know or did you. Can you do something about it? Not really. Uh, so so so I think the problem is also that people are not aware that it's, uh. Yeah. Um.

00:10:41  
*Speaker 1:* So how can you.

00:10:42  
*Speaker 2:* Make the people know that? Okay, here's the iris pattern, but they don't know all the other things that they might also reveal, and actually, nobody does. Uh, because we don't know with what accuracy do we do? We gain this information.

00:10:57  
*Speaker 1:* So how can users be assured that their eye movements data is not being misused for surveillance or tracking beyond the identification purposes.

00:11:08  
*Speaker 2:* I can't. I don't think so. Um, because if they're not aware of it, then then, uh, I mean, surveillance. Yeah. I mean, you okay? You could say that you're using now a camera. It can measure some of your eye movements, but the resolution of the eye is not very large. So some of the details, they can't get some of the information that you get when you do pupil imagery, which is also a reflection of what goes on in the eye. So the changes of the pupil. But most of these changes are due to um, light conditions. So can you filter this away. Most likely not. Uh, meaning that you cannot probably not measure anything about the pupil in the real world because there's so much noise in the data. But actually, nobody knows, uh, how much information is revealed and with what accuracy is essentially unknown.

00:12:07  
*Speaker 1:* So what security measures should be kind of like applied to protect the eye tracking data from leaks or under unauthorized access?

00:12:21  
*Speaker 2:* Can I see this again?

00:12:23  
*Speaker 1:* So, like, what security measures should be taken to protect the stored eye tracking data from leaks or.

00:12:30  
*Speaker 2:* Eye tracking data? My PhD student is looking at this at the moment. So he he's working with the how do we make sure that data used is protected. I mean, you can essentially use standard I mean if the data is not revealed to anyone else and stored securely, password protected, uh, encrypted, blah, blah, blah, all of these things here, they they will also apply to eye tracking data. And when that's compromised, well, all data will get compromised. Right? Yeah. So so so I think for that. Yeah. Then you have the data. The problem is very often. Do you know if if I'm just giving you an iris pattern, you do not know who this person is. You just know that this person a of course it's a it's a leak. But what will you do with it if you don't know what task they are doing? What will you use it for? Uh, you may be able to identify they are who they are based on the eye movements, but most likely not because you do not know what they're doing, where and under which conditions generally. The problem, of course, becomes slightly larger when you're working in extended reality headsets, because there you are constrained much more that than and in more detailed information. Um, I'm not sure what you want to use it for. Uh, but in principle, if you hack into these virtual reality headsets and grab the get the image data. Of course, you can start doing generative models over people's eyes and their eye movements. And that's a security risk. Clearly, clearly.

00:14:19  
*Speaker 1:* So could gays tracking data be used to infer a user's cognitive state or emotions in ways that might pose ethical dilemmas?

00:14:29  
*Speaker 2:* Yes. Of course. Clearly. I mean, I used it for my inaugural lecture, actually, when I became a professor, that there I think it was Netflix or somewhere. I forgot, actually, which company where. It was forbidden to look at some other persons for more than 10s then it was sexual harassment or something like that. But now you have a way of measuring it directly. But the problem is that we can come up with any measure saying that, okay, I'm not allowed to look at Julia at all more than 10s. Uh, but that I'm that my eyes are pointing towards you does not mean that I'm actually paying attention to you. I mean, just look at my lectures. People are staring out, uh, in at the blackboard, but they might be somewhere else on a mentally somewhere else. And we can't measure this from from only from my information. Um, but but but yes, we I mean, there are a lot of things you can infer. How good are you at reading? How much do you pay attention to certain details? Do you observe certain things? Um. Do I mean preference? I mean, people are looking at preferences. What is the people pay attention to, um, such as sexual preferences and other things? Of course. That's this is how you get your information, right. You look at them and as you look at things, you reveal something, uh, and some of it you can't control. So some of it is subconscious and some of it is, is voluntary. And you can. And the problem is that at least. For a short period of time, um, you have no control over these eye movements. And that's what reveals a lot about you. Uh, and I think this is also what people look at, what they look at, personal traits that they have certain ways, micro, uh, gestures that they do, and you can't control it. Uh, and sometimes that one bit of information is enough. Yes. Julia was not paying attention for 30s when I showed this picture of an ice cream.

00:16:48  
*Speaker 1:* Yeah, it's very interesting, actually.

00:16:50  
*Speaker 2:* It is very interesting. I think so too.

00:16:56  
*Speaker 1:* So how could gay striking be used in high security environments like financial transactions or border control?

00:17:07  
*Speaker 2:* Well. It's just another metric, right, that you can use for identification. So given that your the iris pattern matches Julius. Uh, and the password visual password is correct. Uh, while looking at the screen is correct, um, and uh, maximal uh, velocity of your eye movements, which is governed by muscles in the eyes are about. Correct. So, so there are many ways because it's biometric. It's I mean, you can look at it this way, that the eye is a muscle, is governed by muscles and, and is essentially the only visible part of the brain. It's directly connected to your brain. Uh, and it's and so and they are controlled and emotions are controlled. So therefore you have some certainty of, uh, who the individual is. uh. But nothing is perfect. I mean, you can with good generative models, you can model anything. And if you can, then also model the heat and you can model, I don't know, all sorts of things. Then of course you can. You can fool any system.

00:18:26  
*Speaker 1:* Are there any specific cryptographic techniques that can be applied to protect eye tracking data while maintaining the usability?

00:18:36  
*Speaker 2:* Sure. I mean, if you can encode and decode in, uh, quickly, no problem. Who, by the way, who's your supervisor? It's just interesting.

00:18:45  
*Speaker 1:* It's Oksana Kulik.

00:18:47  
*Speaker 2:* Oh, okay. Okay, okay. Of course it is. Um. Yes. I mean, you could use, uh, cryptographic protocols if they're real time or whatever you need. I mean, sure, I mean, it's just encryption of data. The question is, of course, if you really have really good eye trackers that that gives you 1000 frames per second, and you have to do this for very long and send this over a network, then you have a problem. And the problem is also then when you have learned about machine learning model, all the data disappears. Right. So and that's what my PhD is David is looking at is how can you, even with a trained model, know that, uh, this data set, uh, that this model comes from this data set, uh, and, and that turns out to be a difficult problem to solve.

00:19:59  
*Speaker 1:* Ken. Gaze tracking be integrated with blockchain or zero knowledge proofs for privacy preserving authentication.

00:20:10  
*Speaker 2:* Perhaps, I don't know. I have, I haven't looked enough into these things. So, um.

00:20:19  
*Speaker 1:* How do legal and regulatory frameworks such as GDPR impact the development of secure and privacy preserving eye tracking applications?

00:20:31  
*Speaker 2:* We know by I mean all our information is controlled governed by GDPR. I mean, everything you do, you just need to consider it. What do you do with the data? How do you do it? I mean, it's it's a very obvious one. It's like fingerprint times ten or something like this, right. Um, so so it impacted a lot on there, many people looking at privacy and within AI information. The biggest problem, though, is that many of these methods are shit. Uh, they don't do anything. And that is a huge problem. David, my PhD is actually working on a review paper on this. Uh, so he's working on, on, uh, what are the challenges for for this? But it is what people think is secure is absolutely not secure. So essentially, we are close to the Wild West.

00:21:33  
*Speaker 1:* So could AI tracking be used as a multi-factor authentication component alongside other biometrics or behavioral threats?

00:21:43  
*Speaker 2:* 100%. 100%. I mean, if you have fingerprint, eye tracking, facial recognition, uh, hair growth, uh, patterns in the head and stuff like that. Yes. Sure. Absolutely.

00:22:03  
*Speaker 1:* How do you see the future of eye tracking technology evolving as a secure biometric modality in the next decade.

00:22:13  
*Speaker 2:* I'm 100% sure that, uh, that it will continue developing. I mean, I have colleagues that work with meta, for example, on privacy and security stuff. Uh, we work on it. Uh, so, so it must be integrated and people must try to when they develop such tools. So even when you try to sell and meet a headset, they need to make sure that things are following European, uh, legislation. Right. So, uh, so, so I and I think we need to go, uh, that couple of more years before this is really sold, I think. I mean, you can take whatever you have on the shelves on on encryption and all of this. That will, of course, apply. Uh, but I think there are many more ethical questions involved with it.

00:23:08  
*Speaker 1:* Yeah. I don't have any more questions.

00:23:10  
*Speaker 2:* Okay, that was simple.

00:23:11  
*Speaker 1:* Yeah.