00:00:00  
*Speaker 1:* Few in mind. I will send you also the consent form that you can just send me over after.

00:00:23  
*Speaker 2:* This. Just the. Just handle that after it. That's fine. Yeah. Cool. Okay. Well, I'm ready to do it. I assume, uh. Do you want me to start about start talking about, like, what my experience has been? Or do you just want to start throwing out questions?

00:00:41  
*Speaker 1:* Uh, yeah. You can, uh, introduce yourself, and you can just, uh, talk about your experience first and after. I will just ask some of the navigation navigational questions if it will be easier.

00:00:54  
*Speaker 2:* Yeah, sure. Okay. So, uh, basically, I started on the on the cusp, um, doing a reverse engineering of the the name ID app. I that's my bachelor's thesis. And, uh, doing that we learned me and and and uh, my co student and I did with we learned quite a bit about how it works and ended up submitting a couple of things that we figured before they could do better. And one thing that we really thought they should fix. And after that, I basically just took an interest in citizens that we're moving from. Remedy to metadata was also always a lot of stuff changing. And so I took an interest in keeping track of it, basically because that was is the kind of situation where the redesigning the whole thing and, and there's bound to be a lot of problems associated with it, uh, which there has been. And so it's been fun to, to, to find problems with that and also just to, to, you know, challenge myself to understand how it works because they don't really want to know. They don't want people to know how it works for some reason. Um, and so that is resulted in me submitting, I think at this point I'd probably given them 4 or 5 different, uh, books that I thought should be fixed, and I'd say maybe 2 or 3 have been directly fixed after I told them, and some stuff have not and then have been fixed later. Um, and as Carter may have told you, it all culminated with me completely reverse engineering the middle idiot. Uh, and which resulted in them, uh, which they were already planning. They said, you never know if this is true when they say we've already planning this, but they always say this, uh, was resulted in them making it even harder to create a custom app by relying on Google and Apple for validation of their apps, which of course, also prevents people from running it on weird operating systems and stuff like that. So it's it really locks down the app quite a bit. Um, so I've had a lot of experience Just talking with, especially digitally and a little bit with the private companies that they contract with. Um, and where I suppose where the pitfalls are in, in their handling of these social situations. Right. Because ability and remedy is, is a really critical piece of infrastructure. And I think it deserves the security deserves to always be number one when when handling issues from people like me. And I really have done my very best to be in good terms with them, but still, uh, they don't trust me and, uh, they still treat me as if I'm a threat and not a help. Um. So that's one of my biggest complaint is complaints, is that it feels. And this is something that, you know, I can't prove because there's really no way to know. But it feels very political when you report something of of If it's a small security bug that they could just fix right away, then they're happy for it. But if it's not a small security bug, if it's not something, you can fix it right away. If it's structural. Then the gears start. You can feel some kind of political pressure where you know, they won't admit that there's a problem or they will shut you down until they know to talk to anyone, with some with no real idea of when is this going to be fixed? Um, the the biggest issue I think I've had with them was, was when we originally discovered that you could find people's usernames and muted, um, by basically enumerating them. Right. So, so so what happened was, I don't know, did you use them? I'd, I don't know how long you've been living in Denmark for all but the username ID not really. Okay. So normally they used to be a username and password system, a classic username and password system. So you would have to to enter both. And then you would, then you would bring up your little card that you had and then type in a code, and then later on they added an app that you could swipe, but you still had to have a username and code, but then move to meet ID. As you know, it's only a username. There's no password involved. And when I saw that, I was like, what? Because it ruined a lot of the guarantees that you get from a username and password system, because even though it was just a CPI number, you still had to know someone and then start getting getting passwords with the bit of the username. They said it should be secret. But of course most people see a username. So I typed in, I think the first day launched I typed in Henrik was some random, you know, very common Danish name, and it was like, okay, now swipe no no no no no. Right. Because you that meant you could guess people's usernames like that and because of a different change they'd made, but possibly also because of something that we reported to them. And normally if you are typing someone's name into the field, then you cannot log in somewhere else at the same time. And this was this was to prevent you, you timing, timing someone where they think they're logging into their own account, but in reality they're looking into your account. So if you knew someone's username, you could block the from using meta ID. And this was so easy to find me that the usernames you could block, you know, thousands and thousands of people from logging into that if you wanted to. And because this was such a structural problem to the design, right, someone had, I think my idea is that my thinking is that some security guys with the security of metadata, like the structure of the algorithms they use, is actually quite good. And I really like it. But someone must have said at some point it would be very nice, especially for older people, if it was just a username. It's simpler and it is simpler, but it's also very problematic security wise. I can't imagine that anyone except, you know, a front end person maybe, or like a someone who wanted to cook was interested in making it easy to use for other people. Some political decision perhaps. What's the reasoning behind this? So the result was that the whole structure of the whole security of it, the structure of it was compromised by one decision made in the front end. And because they didn't want to change the decision, because now it was already made and it was like this big thing, now you only need a username. Look how nice it is. They ended up having to spend, I don't know how many hours, but they must have spent a long time figuring out how to keep this username system and still make it reasonably safe. So that involved. Eventually they had to implement the QR code that they have now that wasn't there earlier. When you have to scan the QR code of the login that wasn't there earlier, and that's to prevent, you know, me from sending you a login request and you swiping me in. You can't do that if you can't see the QR code. Um, and then they also added such. You could change your username in an app. If you already have an idea, you can change your username directly in the app. You couldn't do that before, so that meant if someone was blocking you from blocking in. You had to turn up at Bowser. This is somewhere in person to get them to change the username, because you can only change. You could only change your username if you were logged in and you couldn't log in, so you were blocked forever. Um, and then they saw that also. But that meant like tons of development time. Instead of fixing the what, what really should have been fixed, it should not just have been a username, but they when we originally reported that I, I think a day or two after it came out immediately, a couple days after I wrote them a long email, I said, listen here, it's a problem. So on and so on and so on. And they wrote back and basically said, well, you can we have sophisticated system. So if you try to execute this at scale, if you don't do it at more than just your own username and you try and block multiple people, it's not going to work. So don't worry about it. And it puts me in a dilemma, right. Because they're basically saying prove it to us. But I can't prove it because if I actually did that, they would probably sue me because there would be an attack on the servers if I, you know, started blogging people, I don't know, usernames. Um, and then I was lucky enough that a year later a journalist got in contact with us and was like, I want to prove this, so can you give me some code and then I'll prove it. And then they actually changed it after that. And but but still claimed that they actually known all along that this was an issue and they would. They were already planning to change it. Uh. Who knows. They aren't very transparent and stuff. Um, but I guess for me, one of the biggest issues that I've seen is that there's still no official ways to report security issues to digital things. Well, not the last time, at least half a year ago. Such when when when the last time I reported something to them was that they still did not have a security incident email, you know, any sort of. So you would have to go through customer service and basically say, I have a security thing, you know, the same customer service that you would go to if you have a problem with your ability. I have some food security leaders I need to report. Can I write it on this email? Who do I need to get in contact with? And they will put you in contact with someone. Or they will just say, yeah, just write it here. It's fine. You know, that's that is not great. And more than that, they are also completely reliant on on the good of people because I don't know, but it's possible I could have sold some of the stuff I found out to someone who were willing to pay more than the Danish government is willing to pay, which is nothing. Um, and when when you're not willing to pay anything and you're also treating the people who are helping you, I would say as if they are as much a problem as a help. Then eventually I think you run the risk of someone saying, fuck it, I'm just going to sell this to someone who actually will pay for it.

00:10:46  
*Speaker 1:* It's very interesting because I read a part of your thesis on your LinkedIn, and it seems to me very interesting. So therefore, I want to ask you, how has Denmark's digitalization strategy influenced national cybersecurity, particularly in the crucial sectors like healthcare and finance?

00:11:08  
*Speaker 2:* It's a good question. I mean, my insight into this is limited, of course, because I haven't actually worked in any of these agencies. But from looking at, I can really only speak from the parts I have seen and from looking at MIT already, especially as I say that it is. What's being built is not bad. There's people that care and they're obviously they're hiring, of course, consultants and such that actually are building good stuff. And so security is being taken into consideration. It really is. But from the point of view of a security researcher, they are not. Not nearly as much as the private industry, private sector. They're not respecting the what they can get from from from from our input. Uh, and they're making it hard to be a security research that wants to help the government. I'd say that's not a lot of, uh, there's not a lot of following of the of the rules you generally follow in security research. Uh. Yeah.

00:12:14  
*Speaker 1:* So what are the main security challenges associated with MIT, ID and how does it compare to previous digital authentication methods such as name ID? So basically, as far as understood your research, uh, narrative for your bachelor's thesis and method as well. So what is your opinion? What is more resilient.

00:12:39  
*Speaker 2:* So so actually the underlying algorithms are almost the same that have been updated a little bit. But it's been you know, it's basically the same code that they've taken and slapped a new front end on top of. Uh, so so I the main idea that we have today is, is, is a lot better than the mid that we had when they faced out. But the melody that existed right after they faced the media was worse. So there was a really a bad period of. I guess the migration period was, was bad and, and and again, they didn't have they really should have been more receptive to, to feedback once they released it, because that's the point where you need the feedback the most. That's that's when you're trying it on new customers. Um, so, so obviously today the biggest problem with mid was was social engineering. It was someone could send you a, you know, a photo of the key card. And if they were using the app, someone could know when you were logging in and they could send you a request, and then you could swipe the request and lock them in. Uh, you can't do that immediately anymore. In fact, it's almost I would say it's nearly impossible to do to, to to unless you, Ironically enough, unless you use some of the tooling that I've built to to scam someone with me already, because the QR codes are valid for 20s. So two QR code QR codes, if you look at the QR code, will lock it and you'll see that it's it's it's actually like a video. It's not just one QR code, it's two QR codes that are constantly swapping back and forth. And every 20s, every 10s. It swaps the new QR code and after 20s any QR code is invalid. So that means if I want to scan you, I need to send you a video of the QR code that you need to scan, and you need to scan it within 20s to actually allow me. And that's pretty hard to do. Unless of course, you just build a website that pretends to be the real meal ID website. And you you. I'm not going to do this because I don't want to get in trouble. But I can send you the link to my, uh, my GitHub here because I've actually built a browser client that basically it's a Python client that does exactly what the Real Madrid browser, you know, piece of process software does. So it creates a login request to your app with a with a username, and then it generates the QR code as an image, as a video file on your disk. And you can scan that and log in. So if you were to integrate this piece of software into a website, you could send someone a link to this and they would get the QR code. You could you could update the curricular code on that website constantly because you can actually generate real login requests using this app. Um, so you could probably still create a, uh, you know, a phishing website using this, but luckily I haven't seen anyone do that yet. But it should be possible still. Um, but but there's the problem is almost always, especially when we're talking about an environment such as a web that is so, so, so free for anyone to play in. It's almost always possible to create, you know, a fake version of a website if you want to spend enough time to, to figure out how everything works and stuff like that. Um, so but but the general gist is I feel like the big idea today is very, very, very strong. But there's a there's always a way you can get around this. The, the protection especially for, for for social engineering is very strong. They've done a very, very serious job of constantly making it harder and harder and harder. And we are further than we were when they faced nobody.

00:16:36  
*Speaker 1:* So how would you comment about the identity self, the issue. So how about the comparison between the name ID and meet ID? So how did it change over the years.

00:16:50  
*Speaker 2:* Which parts are you?

00:16:51  
*Speaker 1:* So how would you comment on the, like risk of the identity theft? The comparison between the named.

00:16:57  
*Speaker 2:* Okay.

00:16:57  
*Speaker 1:* Yeah yeah yeah.

00:16:59  
*Speaker 2:* Yeah. Well for me the again I could just if I knew your CPI number and password which was not easy. But it was also for a lot of people not not hard because a lot of people used to saying then I username and password. Then I could very well just send you a login request and then I could call you and be like, oh, if it's an elderly person, I'll probably say, read me the code of your card. Or maybe they have their. But I say you need to go into the card and and and swipe so, so that I can help you. And they would probably do it and bump you in. And when it came out you could still do the same thing. But but today, like I explained, you can't really do that because you would have to unless they have changed settings to use, because you don't have to use the QR code actually. Then you can use like a four digit code two. But most people will not be doing that because it's less secure and they need to go to like a hidden setting to enable it. Um, you would have to send them a QR code that is valid for the next 20s, so it's not going to work. You're just not going to get an old person to to understand how to do that. Uh, but of course, if you if you know the Midi username and you know the password. They can still wait. No, I gotta remember what the order of insertions is here. I think if you're using, you know, you can get, like, a small code reader as well. You can actually order it for free, and I recommend that to have it as a backup in case you lose the app. Um, it's like a small digital device that will generate a six digit code. I believe if you use that, you ask to insert username, then I think you're supposed to insert the six, uh, digits and then The the password then was then you actually had a password too. I can actually check what the what the order is if I look at my code for just a second. I believe that's how it works. Um. Yeah, yeah. That is how you insert the the six digits first and then the password. And so that means you would have to know what the password is already. You would also have to know what the username is already. And then you can call them and say I need a 62 token. But you can't try and brute force the code before you have a 62 children, because you need to insert the password after the six digit, uh, token code. So, so it it becomes very, very, very difficult, I would say, because you can't be sure that you actually know what the password is before you call them. Um, so my, my, my, I actually I think that idea is very well designed. I just wish they were more receptive to outside help.

00:19:50  
*Speaker 1:* So basically, what lessons can be learned from international cyber incidents to further enhance the security of Denmark's digital identity infrastructure?

00:20:05  
*Speaker 2:* It's a good question. Most times I when I see international, you know, I see the the big leagues where you get like tons of Social Security numbers, leagues in the US and stuff like that is typically systems that are of a much, much, much lower complexity than, than the Danish media system is. So I actually think I think we are we are on the forefront. And I don't think we generally see I can't remember that. I've seen a system that is as sophisticated as the military system is compromised, not off the top of my head, at least. Um, so I think most times when I see that, I think, okay, well, you know, we're still we're still ahead of the curve here because our system is actually, you know, it's a lot harder to to just if you know something, just break it. You actually have to know something and be somewhere and or someone. It's a very it's it's a pretty tight system. It might be. But but of course that all relies on someone not introducing, you know, some coding book that suddenly allows you to log in. They can always happen, but if it works as it's supposed to, then it's a tight system.

00:21:13  
*Speaker 1:* So how do you see the future of Denmark's digital infrastructure evolving?

00:21:20  
*Speaker 2:* So how would I like to see how do I actually see it?

00:21:25  
*Speaker 1:* Let's let's take both the expectations. Yeah.

00:21:30  
*Speaker 2:* Oh, I actually see this that we will keep, uh, we'll keep keeping on the forefront of, of technology because we have been so far, especially with identity based technology, we're very good at it. But we will also keep being very secretive about how it works. And we'll keep we'll keep, uh. Keep paying private companies to do it for us and not really have any sort of expertise in-house. So I would like to see it is, is I would like to see the government hire at least a couple of experts that have to have a lot of expertise in what it is that they're actually running. Uh, and I would also like to see them be a lot more open about how these systems work, but they don't want to talk about how bad it works for some reason. Um, and that's very sad, I think, especially because it is well designed. Um, and, and by talking about how it works and being more transparent about it, you can find more, you know, issues in the system. One of the things I found when I was, uh, reverse engineering this stuff was that one of the. They haven't they they have an endpoint that was only used, an API endpoint that was only used in the app. So that means unless you reverse engineer the app, you have no idea that exists. As far as I remember, it was used when you sign up a new app, and with that API endpoint, a long time after, they made it very hard to find media usernames by limiting how many times you can ask for metered usernames by making it quite limited, made it a lot harder. I find this endpoint where you can also ask for a username that's only used for the app, except it's not limited at all. There's no limits, and that's the only reason that happens, is because someone is sitting in there and thinking, oh, you know, we have this API, but nobody knows it exists, so who cares, right? Um, and by having a public, you're putting a lot more pressure on every single part of the system, even the parts that you think most people won't see and see that you think are better hidden, which is not real security. Of course, you're making it a lot harder for people to to, uh, to exploit that because they were just lucky that I found it and not someone else. That was reverse engineering the app in order to, you know, to break to to compromise some part of the Danish system. And I would really like I would, I would like to see them. I'd really like to see the Danish government making some of the these systems open source, because the point of getting, of moving them to meet the was that it would be state owned. So now the state owns it, but paying private companies to run it. Uh, but my experience when I was talking with them in meetings was that the, the companies that were that were paid to run it were basically the only guys who had any idea how it worked, and they were really not interested in open sourcing it at all. And my I, my, my thinking was I have nothing to back this up at all. But my thinking was that they were probably interested in selling some of these systems that they build to other, uh, states as well, possibly, and other companies as well. And by open sourcing this, even though the state now technically owns it, that makes their work less valuable. Right? Uh, I can't back that up. But but but they they definitely were not interested at all in open sourcing it. And then the people that were actually working in the state who didn't have that much technical knowledge, they were, of course, inclined to believe these consultants, that they paid, that it would be a bad idea to open source.

00:25:04  
*Speaker 1:* So which cybersecurity measures should be prioritized to mitigate emerging threats?

00:25:13  
*Speaker 2:* For sure. I would like to I would like to see the government implement the bounty program. I mean, of course I would. I would like to get some money for what I did, but I don't really care that I didn't. But, you know, in the very best case, they actually have a bounty program where they give some money. If you find a security vulnerability in the government systems. Short of that, just like proper contact points for, for, for for security issues, proper contact points and people that know how to handle it, people that don't freak out when they get served the security issue and don't think that you're being afraid to them, but instead understand that you're being a help and also understand that that you didn't have to do this. And really, you know that this works often out here in terms of like, okay, so I'm saying, oh, well, I found this. I would like to release this in 90 days. Do you have any good reason why I can't release it in 90 days? And then it's like, yeah, you just have to wait. But what do you mean? You can even give me, like, a timeline or anything or, you know, no, no, sorry or something, but, um, so, yeah, that's the first thing that's to get proper contact points for, for, for security issues.

00:26:22  
*Speaker 1:* So how do you see the future of developing like this kind of model of the bounty program. So what will be like ideal outcome to kind of like report the cyber security threat and as well get a feedback.

00:26:39  
*Speaker 2:* Yes. I mean the the ideal outcome is uh, I don't know if it would be, you know, a a portal that basically that basically serves all Danish agencies, perhaps where you can go and you can say, okay, I think this touches this agency, this agency here's my security issue. Maybe that would be very nice, because the government is actually, you know, in a unique situation where they could have a one portal for all the government systems. So that might be very nice, and that might be a way to keep these things centralized such that, uh, they're sure that they're handled correctly. Um, and, and in terms of the bounties, I mean, that this is something that companies do. And I think if especially as you know, as the war is going on, it is more important than ever to ensure that that that there is not only profit to be made if you're on the wrong side. Right. And then that's the that is the case right now. I don't know if Russia would actually be interested in compromising the build system. I assume it's not worthless to be able to shut down the ability for, you know, let's say 100,000 Danes to log to log into media. That must be worth something to someone. But to the Danish government, that knowledge is not worth anything right now. That's that's unfortunately, the sad reality of it. They're not willing to pay anything for that information at least.

00:28:08  
*Speaker 1:* So which I would say like main threats can you point out for now, who are the main threats and what are they and how they can compromise the digital portals of Denmark and digitalization in general?

00:28:27  
*Speaker 2:* I mean, I'm no expert in this, but I mean, of course the main threats threat is Russia. They're the ones that are most interested in actually harming us, so they have the most to gain, I think. Uh, yeah, it's possible, you know, China would be interested in it in some way, but I don't think they have nearly the same interest personally. Um, yeah.

00:28:51  
*Speaker 1:* Yeah. Yeah, I'm done with my questions for now.

00:28:57  
*Speaker 2:* Okay. Thank you. Well, I hope you I hope you got something you can use. Julia. Uh.

00:29:02  
*Speaker 1:* Yeah.

00:29:03  
*Speaker 2:* Because I'm. I mean, I'm I'm by no means. I'm by no means an expert in this field, but I have some unique experiences with the with with the government agencies. Right. Um, so.

00:29:14  
*Speaker 1:* Yeah, if, uh, if possible, can I contact you again for the.

00:29:18  
*Speaker 2:* Yeah, absolutely. I will also be I don't know if if, uh, Carson or I told you this, but I will be at ICU and, uh, at the 7th of March. Oh, uh, to do, like, a 30 minute, uh, guest lecture on the, on BDD, uh, reverse engineering.

00:29:37  
*Speaker 1:* If.

00:29:38  
*Speaker 2:* Uh, so, yeah.

00:29:38  
*Speaker 1:* If you prepare the presentation, can you please send it over?

00:29:43  
*Speaker 2:* Yeah, yeah. When I've I've done it, I can say I could certainly send that as well for sure. Yeah.

00:29:49  
*Speaker 1:* Yeah. And if it's not a problem, can I use some of your information from your thesis and the back end.

00:29:57  
*Speaker 2:* Oh yeah. Absolutely. That's that's public knowledge. So you can use all that is one as far as I'm concerned. Anyone can use that now.

00:30:04  
*Speaker 1:* So yeah. But anyway I wanted to like get your permission like not to like violate anything.

00:30:12  
*Speaker 2:* Yeah. Go ahead.

00:30:13  
*Speaker 1:* Yeah.

00:30:13  
*Speaker 2:* Go ahead. I also think it's interesting because it paints you know, it clearly talks about some of the stuff that was wrong before that is no longer wrong anymore. So that is improvements in the security right.

00:30:26  
*Speaker 1:* Yep. Yes. Yes. Thank you a lot for uh, for Percy in my interview.

00:30:34  
*Speaker 2:* No problem. And good luck.

00:30:36  
*Speaker 1:* Yeah. Thank you so much. Yeah. Have a nice day.

00:30:39  
*Speaker 2:* Have a nice day.