### Security\_week8\_lec02-20241029\_14:50

说话人1 00:00  
Valerie is responsible for choosing this long strike that you can choose it as far. That's the one that has it before. Therefore, Valerie would have taken place to Alice. Right? If we kept it the way it should have been, it should have been signature b of ten, five, and eight, and that you would not be able to. This is quite an advanced thing, but it's an interesting thing, because it shows like, if you read the protocol specifications, even if there's like something that is very minor, very small thing, right? This is the order of some things. It's generally got a good idea to change. Is it might not look like in any way that it's significant, but it could actually very seriously affect the overall security.

And then we get to the last one. So let's say we have a really complicated protocol, many people, lots of messages. What do we do? Right now, in this case, we have others. We have four, we have a third party. In the next lecture. We'll talk a lot about third parties, right? Alice is sending to this s our identity box identity in a random number, s sending back to Alice. Alice is rather than number four sided. The tab are all encrypted with tas and what's also in here is this is for Paul. This is KAB the identity of Alice interpreted with TPS right? And then Alice seems to form the message that is the same to her, that you just call this message, kmb others as well. Bob will then create the random values and Alice encrypted with pab Alice will send ab minus y contributed to KAB yeah.

说话人2 02:03  
Before.

说话人1 02:03  
So this is quite a complicated thing. Right? If I told you to look at this, i'll give you a couple of minutes. Think about who is a pink character, who right? Who are the system is indicated to guys, not three parties. There's another dedicated to this. It's not as if they get to be. It is a dedicated, right? It is a dedicated to be. And it's be as any kind of see what you think. What do we think? The way that you solve this when you think about this Information, is that having many different parties doesn't really make it much more complicated, because identification can only really happen between two people and 81 partners. You can just make tears. You can say what happens between a and s what happens between a and b what happens between s and as and b what happens between d and a and DNS right.

First of all, we can say is analysis dedicated to this? Yes or no? What is the message going from Alice to s early mistakes. It goes at this identifier identifier being a random number.

So Alice is not authentic anyway. Is this indicated to a it seems to add a message that only somebody with tas can make. And inside this message there is Alice's knowledge. All right, yes. I guess it was benefited to others. Is Bob is dedicated to s this is the easiest one, yes or no? No, because it's never even the basis from 13 days. Right? So what about this? Two ball? This is a little bit interesting. So it does it for the message. Is this pab Alice's identity and pba in theory, only is sort of like this message because he uses, yes. But there isn't really freshness in it, right? It doesn't have announced involvement. There is this new key, but that doesn't really guarantee freshness, because ace chose the value. Right? It doesn't really prevent us from replaying and reporting it and saving it to form later. Right? I miss Bob keep some long log of every single message of cases in the city. So that's what we online. This is not really a thing you played before.

At the end of message three, Alice now has the new PAD and Bob has the new PAD right? Bob chooses a random number KAB and sends it to Alice. That's the early message of boxes to others. Is that enough to indicate involved to others? Do we have data origin of education? Is it something that only Bob can do? Yes, the only one can encrypt with dnd in theory is the only other person who is key.

But there's no freshness even though there is a loans if the person says the loans and encrypt it, that's not precious. The guy that's trying to prove that it is the person cannot generate the revenue. Right? Because that doesn't work for replay protection, right? Because then I just record this and I send it tomorrow. There is a random number in it, but it's coming from the syndrome. Right? For a random number to work, Alice has the same that random number of the ball. Bob has to include it and say that then Alice knows this is fresh, because this is my random number. If Bob is just in charge of sending the random number that doesn't work. Logical concepts are different than we have counted, right? This is a random number, so actually bothers what are they getting to that? Is that Alice and then you get involved? Yes. Because this last message as nd minus one, kad so basically, it's something only Alice can do, because she uses PAD and has nd minus one, and then which also illustrated the palace would be true this message.

So we definitely getting this message from Alice as freshness in it, because there's a new random number that has been seen by Bob.

Ensure Alice is not a dedicated to this, but this is a dedicated to Alice. B is not dedicated to SS is not a dedicated to Bob. Bob is not dedicated to Alice and others in the indicator involved, right? But we can solve all of this by just looking at tables. I can see what goes between them.

That is the end of your vacation lecture. It is 3 o'clock, so we can have a long break. We can have a 10 minute break. And then when we come back, I will start talking about 50 minutes. You

说话人2 09:52  
get up. So what's I get up? Yeah. So you then, what is that job? Can you but nana, same as a machine learning supermanship, choose peace area, the radio thanks to the show so far. I don't know to told you. I so many of them are so many help looking at all. And it isn't true. Such as I don't think it should be almost it looks. I got you. So it is. How was it? I I you don't know, it would be the right thing, which is a man.

Nana. They are gonna have the job. Do not do it. It was instead of English in the opinion about you can also send me to jobs in a team or couple of that is just this is psdk for now what you mean is sort of winners level can I include? So we don't work it out. Person has you there. And having a little bit here time with all three of the secrets, are we going as far as that meaning and so on? The survivors is it, but from the normal. I think it is good for us. Yeah.