### Security\_week9\_tutorial-20241105

说话人1 00:01  
Very good communicating to trust the party, to be a hierarchy. So basically, covering all that, what we did last week, just big provision we talked about the establishment. So the establishment is the process by which we give people these. So people need to use keys, we generate them and we give it to them. And the process of sharing, these is basically for the establishment. These two big concepts we talked about and one was key control. So who decides what the value of the key is going to be? So when we have key establishment, we always related to alice involved, even if there's other people involved, we look at it from their perspective.

All right. If alice can decide what the key is going to be, or bob can decide, then that person that decides by themselves have key control. Any protocol that looks like that would be key transport. If alice and bob decides together or alice and bob get somebody else can help them to do it, and then other person decides on whether it's going to be. Otherwise, alice and paul has no involvement in what he is going to be. Then that is the agreement. Because alice and bob or alice or bob do not have to be controlled. Then the last thing we talked about the ski confirmation. Remember, we said the proclamation is how sure alice and bob is at the end that the other one has the key. Essentially, even the protocol itself, the new key is actually used. That is explicit key authentication, because not only do they think in theory that it should have happened, they actually show each other that it has happened, right? Or in some cases, if the new key is not used in the protocol, then we call it into secure indication.

So when the protocol ends, they believe that the other one has a key, but the other person has not actually showed them. That is the case. We also did add some different models, so we had the direct v communicating entities are just others involved, but then we also have the trust of third party, the trusted type that it would be a translation center if the protocol is doing the transport.

In other words, alice has a key once you use the key with bob, so alice sends the key to the translation center. The translation center seems that before, all right, we also said that bob doesn't have to be online. Bob can just be connected to others. Alice, without the key translation center, I want to use this key before the key translation center will give a message to alice, that she can pass along the ball that would allow for to have that key. Right? Alternatively, we could have a key distribution center, which is key agreement. In other words, here alice doesn't have a key. Bob doesn't have a key, but they want to talk to each other. Alice tells the kbci need a key. The kbc chooses the key. Alice involved does not have key control, sends them in the key to others, sends the key to all. All right. Once again, both does not need to be online. So alice can ask the kdc to give it a message. It was involved so that alice and paul can end up with a shared key.

Okay? So for question one, the following protocol establishes a new pad between alice involved using a trusted third party is what type of key establishment is this and what is a school. So alice seems to is, here is a key idea. I I want to use it with ball, and it's encrypted with a key shared between others and the trusted third party, as it seems to be a message that is espad you should be using it with alice, encrypted with the key shared between growth and then cross the third party.

This is an example of key transport, because alice clearly has key control. So alice chooses pad she transcends it to the trusted third party. And the trusted product sends it to all. It's essentially, this is what's happening here. Exactly this protocol. However, since gab to abcabc sends, he bought the ace in this case. Thanks. Right. This makes is a key translation center. Right? Question two, consider the following protocol where e is symmetric encryption algorithm. K is a long term symmetric kitchen and others involved. This is a mutual indication protocol and it seems are one ball. While we encrypt r one's into vector alice along with r two, alice in groups are too vain at the ball. So bob has a message from alice, expressionist and data origin of education, phrases from the non state origin, and then you get it from encryption. Alice has a basis from form that aspiration is that or in the mitigation.

So alice involved a mutually the same debate. Right? There's a scheme support any key agreement or key establishment, if not modify the protocol so that it does. The only way we can really do the establishment of this protocol as is is if we use r one and r two as some input to generate the key, the only problem with that is that r one and r two is currently public.

We went off to say something like the key is the hash of r one and r two. That means everybody has the key. Actually, as a threatened year, the protocol cannot support any type of ehw so the easiest way to change it is simply to take the second message. They basically include in a key dash, which is the new key that bob and alice wants to share. In the second message, it's the encryption of r one. We can add rp we measure and a dash. Fox, it is the alice. And then alice in the last message been confirmed involved that she got paid out, she can also leave this out. In pierre, you want. What is the implication of this aid as actually being seen back involved? It is explicit key of the implication, so it's a form of key confirmation.

So alice actually shows bob, I have received the fee. I confirm that I received. So this protocol is a key transport of the agreement, so this is key transport. It's really involved the size of the value of the key, encrypted and sent it to. Alice can use a key. They call exercise ok for question three, consider the following protocol where he is the symmetric encryption scheme. K is computed as d to the ad mod p and square brackets of the message. Name means this message assigned by the measures indicated by the name. What is the long term secret of this scheme? So we said that if two people as involved 12, establish new keys for themselves, they need some kind of existing, secure relationship. They need a shared key. They need some private, private secret that they can use the base, the security of that establishment.

This method uses just the hormone. Essentially, this is using probability for third manage a new, symmetric key. So we using the open, established and used to make a shaky. So we remind ourselves of the helper alice into the a one of the four boxes, g to be more alice. Bob takes b to the, a mod b raises it to the power b and educates d to the b mod b raises it to the power a and alice and paul both end up with g to ab for t okay? We also know that this doesn't work, right? Because we said it's vulnerable to man in the middle of time. So we need the extra data origin of indication. This extra data origin of education comes from the signatures. Right? So alice will send her the behelman component to bob. Bob will say he is the behelman component to alice. You will then sign the different message from alice and the different company. He said himself, alice can verify the signature and see that treaty has not put anything in the middle.

All right, with the treaty can say g to the p mod p involves instead probably not assign g to the p mod p when alice takes the ckto to realize somebody else do something there. Right? And she encrypts this entire thing with the new key tape. Right? Then finally, alice will send back the signature of g to a one, d and g to the d one g as well. The ball players, it's no one has missed a run with the data between him and us. She also encrypt everything with the new uk so this is an example of key agreement, because alice involved users, if they help them, others chooses experiment a or chooses the exponent b and exponent a and b contributes to the new key judging.

So neither of them has key control. So it's the agreement, right? Both of them hearing the protocol itself uses the utk we also have explicit view of indication when we thinking about the confirmation. But patient is asking, what is the long term secret of the scheme?

If we look at the development of g to the a one, bg to the b one, b a is a secret that other people don't know, and b is a secret that other people don't know. Gnp is public. But despite a and b being a secret, it's not a long term secret. It gets generated every single time we run the protocol that we had a support. So we can't really use a and b to provide a long term secret between the two. Then we have this ek kpak is a secret that only no violence of all the only problem is that only generated enough. It's a key that the protocol is actually made.

This is also not the long term secret that allows the relationship between others involved for exchanging. So the only key that is left involves public private repair and alice's public private repair. For this protocol to work. Therefore, the long term secret is basically, especially analysis involves privately. Bob has a private key, alice has a private key, and bob has the corresponding trusted public key for others, and others has this prospect, public key for both. There is ease is the relationship that alice and bob already hires that allows them to securely the savage they need.

The answer would be the long term secret of the scheme is the private key of others and the private key of all anba random, gnpo public. Decision key is new with this secret, but it's new. So the long term secret is the part inside. Right? So last question, last question is kind of important, because it is something that you must be able to do. You must be able to design your own protocol, even a set of constraints. Right? What the question is, design a protocol that will use a key distribution center to set up a shared pk between us involved. You should use time stamps operations and assume that all cannot go directly to the kdc alice involved does not need to be as indicated to each other. And there is no need for because it gives education, state, all your assumptions about the system. So from that, I sort of underline the important bits that it's a key distribution center. This gives you an idea about whether the protocol should be key transport for the agreement.

All right. Usually these time stamps of gracious, it seemed involved kind of go directly to the kdc so involve not being able to talk directly to the kdc means that we are basically believe for something that like this.

This is not giving you information about what the protocol and the architecture for the protocols to apply. Alice above does not need to be dedicated to each other, and there's no need for explicit, give any patient in terms of what that will means. He distribution means, right? For others involved. It means others involved doesn't have to be controlled. It needs to be a key agreement protocol. So it does say that alex and bob does not need to be dedicated to each other, but who should be dedicated? The kdc if the kdc is going to be keys to others involved, the kdc has to be dedicated to others involved this. Do you need to use your kek in the protocol? No, because you only need implicit. You have any patients. So how does involve does not actually have to use ukk why the assumptions are there for those who work? Alice involved shares keys with the agency?

Okay? Assumptions are actually very important, like assumptions. Insecurity is very important, because we generally design systems to work only for a particularly sake of assumptions. We make assumptions about the attacker, we make assumptions about the parties and what they can do. We make assumptions about what can go wrong and how we can fix it. Your assumption is quite important. Whenever you design a protocol, you have to write down your assumption. How does what do you think? Might say I designed the protocol because I thought about it in this specific way.

I assume that Alice involved has this shared key. I assume that have shared time clock, all sorts of things. The other thing that's not explicitly mentioned here, but if you give a protocol answer in the exam, you can also define your own notation. Right? This is important. You should say I when I put encryption, underscore a 30 bracket, that means it's a symmetric encryption with key pay. If I go and put square bracket, sine a it means everything in this geographic is signed by a right? That means you don't have to remember any notation. You can use any notation you want as long as it makes sense, because you don't find it. Maybe you do not. Okay, so why does this standard look like? Bob will say, I want to talk to others. Alice will tell the trusted part and I want to go to the ball. The trusted party was to make two messages, one for others, encrypted with the key, a chair to others, the same with the key and shares with ball pppapapapp inside the message, there will be a time stamp, the key value that others involved should use.

And the person that they should use the key word, as is the five step is if you pay and eligible, involved is the 5 % here to be paying a policy for us.

All right? That's the third party status. Alice and Alice keeps the first message and send the second part of the message, evolve as everything we want to happen here. Trust the third party should be dedicated to others. It is because the expressions from the front step, is there the origin of indication from the kap president party is indicated involved? Because it's creations from the time stamps. These data arguments and education shared on the encryption. Right? It's not as PK four times PK and PK was decided by the trust of the party. So how is involved does not have key control. Alice involved that they use this in upk but they don't need to because we only need because it there is no need for explicit key of the Information. Right? And there's also no need to indicate highly simple with one another.

Okay. Next up is what is the key hierarchy in this protocol? How many levels are there in the key hierarchy for this protocol? Remember key hierarchy, we said we have different labels of keys. Some keys are most important. They're at the Top. That is the loss of key. That's only used to make other keys. And then your key at the bottom is the station key. That's the one that people are actually gonna use. We talk to each other. This protocol, how many neighborhoods of here? Two, it is the last key, which is the Kat and the tvd which is a key that's only used to make new keys. Then there's ek which is the station key, which others the ball is actually not going to use for whatever they want to do. Right? Remember, the idea is that we use this key ka lot for everyday things we use. This. Two key is very rarely because to establish them initially, probably quite often ok so the second question is, it's arpk that we are agreeing on or establishing is that 256 bit ASP but our two keys here in PPT are only 56 bit day speeds.

Alice involved establishes the new key using this for 5013, fifteen. After they have the new PK they're going to improve some data using a is to six. How much effort does an attacker need to find ek we know that to report search and e is two to the n minus one, the brute force search PK would be two to the 255. Right? Would that be correct? Or is there easier way to do this? If we are interrupting ek with tat and tbt and tbtatat is very short. A smart attacker would not search for pay, because if they search for tat or tbt which are only 56 bits long, and they find them, they can think of this message and give pay.

In this case, what happens is if we design the protocol in that way, it's all nice that the ek is very long, but its effective security is only as strong as this one and this one. Right? So that brings up another point about key hierarchy. So we said key hierarchy, the upper keys, I used to only generate the lower level keys by the lower level keys, also inherit the security of the Top level ones. If I take 5,000 of key, I'm sharing it with a tainted key. My effective security is only the tainted key, because that is the weak . in the system. Right? If my master key is dangerous, as long as my position is a thousand, no one's going to search for that one. They're going to search for the last feet, and then just the equivalent find 1,000 point.

That means if we do the establishment, the longer he should always be at the Top. If I have short keys at the Top and then put Top keys at the bottom. Because the bottom ones will inherit the strength of the upper ones. If anything, you can go the other way, right? You can basically say organization people that may be quite short, because we're going to use it for a very short amount of time. I miss the Top of data is pretty much useless and I can find it tomorrow. But even though they can later, they can find the short key by the time they do it an hour from now, a couple of minutes from now. It is not useful anymore. Our station key is to possibly be a bit shorter if we really have. Right? We cannot make our loss of peace shorter, because that will stay at the security level. 435, something. Right? So that is everything for the tutorial. And the tutorial solution is on canvas. And so is the extra notes. For the year discussion lectures. I'll see you next week, and we'll start with computer security. Thank you.