### Security\_week8\_lec02.2-20241029\_15:12

说话人1 00:00  
This we prevent replay attacks. Replay attacks is, if I just send you the encryption of a value, then clearly I have made that message, but there's no guarantee that I have made this message now. So somebody uses that message to dedicate to you speculative brought on that basis for me many years ago, and it's not just saving sdu so the basic must have something there all gracious as well, right? And we look at some protocol examples. We looked at unilateral we show. And we also looked at that additional problem if you have and data origin of education with symmetric crypto, which was the reflection attack. Therefore, we said, generally, we solve that we always try to indicate the direction of the message as well by putting the updated fire of the receiver into the message.

In today's lecture, we can then look at key management. The key management is not a security service, but as a security area, you could always argue that it's one of the most important. It's not very exciting when you understand it, but it's incredibly important.

Up to now, we've had a nature on symmetric encryption, on asymmetric encryption, on data integrity. We talked about all these wonderful things. Adsrsa max has h max, cbc max digital signatures. We always have to assume that there was key material available for those things to work. Right? Key management relates to the entire area of security engineering that ensures that the people that need them have the appropriate needs. Right? Long time ago, when we talked about physics principle, he said, everybody does everything about everything, except people should not keep. How do we generate these key security? And how do we give it to the people that need to use it? Okay. In this lecture, we look at two different things. We look at how we manage the matrices. In other words, how we manage e sports of matrix of the systems. And then, finally, we'll see how we manage asymmetric ease or public key significance, which is the most common way to do that.

Even within the symmetric key management section, we can manage the matrix keys using other symmetric key systems. Prefer systems, or we can manage the matrices with asymmetric keys. The goals for today is to look at the different concepts of managing a symmetric key, using symmetric mechanisms. Then next week, we'll move on managing symmetric key with asymmetric crypto and managing asymmetric is as well. So in terms of key management, just like in the previous lecture, the school, this lecture is actually based on the standard. It is standard. I saw 11770, which is the security techniques for key management, understand it, and we will be using the same technology and you will be using the same protocol examples. Yeah, so the management as described in the standard is actually a very, very big area that involves very many different things.

First of all, we need to know how to generate at it's a matrix key. This is basically making a random bit street, right? That is difficult for other people to predict. Or publicly prefer. This might be a little bit harder because you have to choose a variety of things.

So that, for example, for out of all, you need to generate there, you need to do some crimes that will works. For rsa you need to choose the two primes, and you need to choose the public exploded directly so that it's relatively prime to the fire, then all sorts of things. And this is our key generation does. Right? The second step is key establishment. So the establishment is maybe the main part of the management and what we will focus on in this nature. So what does key establishment mean? So once we have made the key, we need to give that key to the person that needs it. So that process of giving the key or installing the key with the person that should use it is called establishment.

So if I make a key, and then I send it to alice, i'm establishing that heat by sending it to us. More likely if alice and bob wants to talk to each other, they need a new key that process for them to make a key. So they talk to each other. It is called the establishment, right? Basically exchanging the keys between each other. We also need to consider how to secure restore the key. This might seem obvious because it's something that is very sensitive. So we have to put it in a secure place. But there's a lot of practical problems involving humanity. Right? For example, what is the device that you work on is not very secure. So for a long time, we had no followers. As all this fancy is today entirely because today whose trusted execution environments, we can do lots of nice security things, quite securely.

But the big thing about mobile phones was that they insecure, right? They have a memory space that a processor that only absolutely on them. They don't really have a proper operating system. The operating system was sort of made by the handset manufacturer. Now is supposed to have apps that offer security, but like waiting for the key. You just put it in the code, restore the memory. Other process has been deleted. What is going on? Right? These days, as I said, these nice classic execution environments across the memory where you can submit memory would be the production, where you can security store things and hardware is in a very somebody tries to act on your phone take part. The key is secure.

There's also other people with cheaper applications. This simply say, i'm gonna keep my key in the class, so the key is never going to leave back in where it is secure. The application on the phone is gonna be really the front end displaying things to the user. But the key actually doesn't go to the five, right? So different things we can think about different things. And then that same problem happens a lot of things now that we will go from. We also need to think about key backup. I make a key. I encrypt all the data in my company with this key. I have a little bit of a crash. The key gets corrupted.

Now I can get none of my data back. This is not a good idea. We probably need to keep a copy of our e seller. But this copy of the key, we also need to think where we had scored, because it has to be scored at some place that is secure. And then it's not gonna be affected with the original key rights, all sorts of things. Right? So basically, some of this might be quite valuable. So you might actually say we have a secure disk somewhere or a type of proof, usb drive. And half the key is on that and kept by this guy. And half of the key is on another usc drive to get $500. So really, when something bad happens, these two guys can get together. Put the usb stick into some device at the same time with them, like they do in old movies when they have a computer, when they are ready secret door, this key can be reconstituted and we can get it back.

But none of those people have access to the actual role key. Then we need to actually use the key, right? So if you get it out of stories, we use the key. And when we finish using the key, every single key is supposed to have a defined life cycle. So no key is supposed to live infinitely for the rest of time. What the standard actually says is every single key that you made should only work for a safe time period.

And then it should be changed. The key can be changed because it has been compromised, because somebody got hold of it that she did, or if he will change when it gets to the end of his life, basically, it would be its expiry date, right? When it gets there, we have to change the key. And then the process starts again. When we stop using the key, we need to destroy it. So there's no one else ever finds it, or in some cases, we might need to keep it. For example, let's say we have a public private key pair. We signed a lot of documents with it. Now, the private public key pair comes to the end of this lifetime and it is expired.

Now we are going to generate a new signing fee, but there's still these documents, both in iran. Then we have signed and we might have to verify that we, in fact, signed them. So we might have to occupy the public key that we can use to verify those documents. Right? And then you can destroy the final. Right? So this is the big story with key management, and we can only do at this part. Right? So in practice, usually your keys are kept in a special device, which is called the hsm are the security model. It's basically like a very special server. You can get it in various form factors. The bigger ones are basically rack servers. You can put it in a as computing center. Right?

Now, also small ones that you can plug into servers. So like an expansive time at the graphic style connected with it inside the machines, and then it will be management for you. What is special about these things? And they're completely trusted hardware. They are very secure hardware box. They have lots of hardware security measure in them. For example, if somebody tries to turn the whole of it, it will immediately erase everything. So there's a lot of hardware security measures and software security. Right? Usually they are connected into the network like any other secure server you can connect, then why I would say what pls and they can basically security communicate with everything else, right? They're also quite impressive. They can do almost every security algorithm. You can think of asymmetric crypto signing and encryption, symmetric concern, encryption in mac. The new hash is in the heat derivation. And if you do good quality random number generation. So most of these things, if you buy a good one, can actually do two random number generation.

So in other words, again, it has an internal, electronic or physical process that it can observe to basically make perfectly good to random numbers. Okay. So you give a bit security architecture and the rule. You'll see these very often. Maybe there's a knife on that. If anyone ever asked, if people to do security audit, right? Sometimes people say, can you come to the integration? Basically, that means I came to my sister. That's one thing. Normally, when people say here's an occupation, then you see if the architecture is okay. The main thing people want to talk about is the hsa and the security management always ask is my key long enough is my tv longer in my tv life cycle gone too long? Should I make it expire? 2 weeks. They got 2 years. Right? So as I said, it doesn't sound very exciting. It's actually really important in my systems as a whole secure. It doesn't matter if you have a basic up there in your key management is.

Okay, how do we manage symmetric keys? The section that we are going to do today is how do we manage the matrices using symmetric key topography? Right? There are three models in this system and you can define protocols for each. We can consider directly communicating entities. In other words, alice involved coping to each other. There's only an alice in the ball. We can then talk about two different models with this. Alice involved plus a third person. That third person is the trusted person that can help them generate this piece that's referred to as the trusted third party. Right? And trusted third parties can operate within two models. The transit third party can be a key distribution center, or the transit third party can be a key transformation center. Right? So what directly communicating in peace? We don't have the stress of third party, so we have others. We have four. And basically, alice and bob needs to talk to each other. And in this process, they have to securely exchange a new key.

This is quite important when we talk actually about key establishment, all of the models that we have misuse that there's already a relationship between the people involved. In other words, here, alice and bob does not start off knowing nothing about each other. If that is the case, key establishment would be extremely hard. Right? The assumption is that alice and bob already has a shared secret key, but they want to make a new one how to make that first initial secret key exchange is sometimes not very well applied. All right? And sometimes that is manual process. Alice and bob will have to get together. They will basically have to be a person that goes between them with a piece of plastic hardware to put the key analysis. That's key involved, so that initial key is also extremely valuable.

We will talk next week when we finish the section of the major keys about key hierarchies. Right here, hierarchy says that the top is a loss of key, which is the very first key that alice involved establishes. That is so difficult to establish because it only has to be done manually every single time. The alice involved doesn't really want to use that key to do everyday business. So alice and bob will use that key to make other keys to the everyday business, but that key will be used very little. Because the less we use the key, the less likely it is to get it back. So we can need that key for a very long time. Its life cycle can be extremely long. Whereas for the keys at the bottom, the life cycle might be a minute, right? Whatever. And then we can make anyone. So just remember, the key establishment is always even with the trust of the parties considered to be between two people, between others and both.

The trust of the parties relates to distribution within a domain. We have two possible cases. We can use asymmetric techniques, which we'll look at next week, or we can use symmetric techniques. So in other words, we can have a transitive party, but the transitive party, alice involved, can still use the matrix method to exchange being used to the repeat. Right? So for the second case, we didn't have this key distribution center for this key translation center, for the key translation in the key distribution center, alice and bob already need a relationship with that, the problem.

So when the system starts, they already have a shared e with their trusted 35. When we have this distribution within the right, we have the key translation center. We have this entity that transports keys between alice and bob. And if we have a key distribution center, we have this entity that make sure that alice involved agrees on 18. So this is the terminology. So there is a difference between transport and agreement. So just if you look at the words, it sounds a little bit like if we have transport, one person already has the e and we are taking the same copy of that e to the other person. Whereas for key agreement, that probably means no one has a key, and they are talking and negotiating a little bit to find the key. Right? And that would sound sort of right.

So we have the key translation center. What will happen is we have palace, and we have all, and we have the stress of third party, which is the key translations in alice has a relationship with the kbc paul has a relationship with the kbc already, so they have to share team with each other. Right? Alice will tell the kbci have, I want to talk to paul. I already have a key that I want to use to talk to paul. Can you help me give this key to goal? So our sense is key to the key translation center. The key translation takes this key and sends it evolve. Now, lss the key. What has the key analysis more than for the other key? Right? These models can also be slightly different, or can also be a person that cannot directly predict to the kpc otherwise, bob can be offline, but what can connect to alice, in which case alice becomes its connection to the kpc okay?

In this case, alice will say i'm here with bob. I want to talk to bob. Can you help me give the key to paul? Alice will give the key to the kbc the kbc will then tell alice here is a message for paul, pass it along to bob. And if you do that, bob will also have the key. And bob will be able to talk to you.

Where is this useful in practice? This is useful for anything where we need prepare between others as well, but bob is maybe not a very fancy device. Right? Think about bob is maybe a smart card like a credit card. Right? The credit card cannot directly connect to the internet, cannot connect, directly connect to the translation center. As this is a credit card machine where I want to use my card to make a payment. If that part gets put into the machine, now that part is connected through the machine to the trust of the body. Right? The machine can then tell the trust of the party. I've got this card here. I need to make a payment transaction with it, but I don't share it with it. Can you please send me a key or a message that I can pass this card? So we end up with a shared key, and the message will come back. Alice will they pass the basis to the card can be encrypted.

And then basically, the card and the credit card machine can talk to each other. Right? There might be some other needs for this model as well. As you say, as simple as the point that we can be done. Right? The next model is the key distribution center. Remember, for key translation, we have transformed, we have to skip it from alice before. It gives you distribution center. We have key agreement. Here, alice above does not start within the simplest model, is that alice, without a key distribution center, I want to go to ball that I don't have a key to go to ball. Can you help us? The key distribution center will say sure the key distribution center will then make a key, send that key to alice, and then send that key. We got right. Now, once again, alice has the key and all has the key, but it's not this process of transport where the key is already there and it goes to values involved. This guy is somebody else that is not as involved, decided on what this value was going to be.

Okay? We can also have the offline method, right? We can basically say alice is connected, involved was not able to go online. Alice will often keep this mission center to make them a the key distribution center will send two messages back. One is intended to alice. What is it needed for all? Right? And basically, once alice has received her message and formats received his message, they can both prepare message. And basically, now they have a shared secret. He, okay. Now we have talked about a lot of things. What is the value is we can come back to the things that we mentioned or discussed and try and sort of only write down what they need. So the first thing is key establishment. The establishment is this entire process of once we have a key, making this key available to the people that need to use the key. Right?

The next thing is key control who has the ability to choose the keys value. Right? The key control is important because it determines whether we are dealing with key agreement, or we are eating of heat, transport, heat, transport is. Alice already has chosen the key that means alice has to keep control because alice alone decided what that key value was. And then the key transport protocol also said that he involved for key agreement, neither entity has to keep control. Right? So alice doesn't choose with the value of the years. Bob doesn't choose what the value of the key is. Alison paul might contribute parts of the key, but none of them are the only one of them responsible for making that decision.

That's why we could have something like the key distribution center where alice doesn't decide the value of the key. Bob doesn't decide the value of the key. They are the center decides the value of the key.

Now neither for or alice has the control. And that's an example of key agreement. Right? If we want to think about that in, so it's like a different way. I if we basically have a coffee room or a break room, and I installed a key there, which is like a keypad, I choose the intricate to be 1234, and then I send an email to everybody else saying they're coming to get into the break room as much as before. That would be an example of heat transport. Right? Because I chose the value of the key, i'm not going to use the key myself, and i've given that key to everybody else. Right? I have decided what was going to be.

Alternatively, if I go somewhere to highway store and I buy an actual lock, I say I just need to secure this room. Can I have some key copies of the key? And can I have a lot? Then that is almost as simple example of key reason. Right? Because basically they not trusted the party. The guy at the hardware store, he's choosing the law, he's choosing the key, and he's just making copies of the key, which he will then use to me. And I will pass along to you. So I don't actually choose whether he looks like guy that I guess so chooses with. He looks like, but I ended up using it with anybody else. Okay? That is simpler. Explanation of that. The final thing is key confirmation, so assurance that the other person actually has the key. Right? What does this mean? There's actually two different levels of keep confirmation, implicit, give indication, and explicit, give indication. So what does keep confirmation mean? When we run the protocol? We assume that at the end, alice has the key, bob has the key.

So from alice's perspective, with the protocol finishes, she wants to have some idea that the only other person in the system that now has the key is for rather than bob successfully received the eve, and then bob is the only one with the key. Right? So basically, if she thinks about implicit view of medication, alice basically says, I looked at the protocol, I trust the protocol. So when we are finished, i'm pretty certain that bob has the key and that bob is the only person with the key, but i'm not 100 %, sure. And explicitly of the invention, bob will actually use the new key as part of the protocol. Right? So in other words, now alice is very sure, right? She knows that the protocol is secure. She knows that the key could only have got involved and actually also sees bob using it as part of the establishment protocol. So nasa is really sure that bob has it.

Once again, if we try to look at a slightly different example, right? If you buy your friends, maybe a gift, you send it to them by a career service. Okay? So you ask the courier service, you don't think there are this on this. So you track it online, and then the status say that this package has been delivered to this address. There's like a little thing that looks like a signature.

Okay?

So now because you trust the courier and the courier service, you now have an implicit idea that your friend has got the package, because nearly the korea went to this address, you specify that somebody there made a signature like a little sweet evening. Right?

You are pretty sure this will, but also you're not definitely sure, right? Because it couldn't be like the guy in the apartment makes good or they could have gone through the romantics. We don't know, but we have an issue of it as part of the comments. Either of your friends are messages you with a photo of the gift and say, hey, thank you. I'm so happy that I got this gift. Then you got 100 %, sure. Right? That is the same here. That would be explicitly sure that this gift was received. So we just think about this gift is a key. So when we trust the process, that's the only thing we could do. Then at the end of the process completes, we have implicit youth injection. If we have the process plus the other person actually uses the new key, then we are absolutely sure. Then we have explicit give information.

Let's look at some examples. Special one is the establishment example six from the standard beginning six. It's for directly communicating entities. Alice involved must share a secret pkb rarb announces a if we are key material. Right? Now we have bob sending rb to alice. How does things back? The encryption of rar evolved some key material. The stakes feel like a sort of education converted to be anything, involves sends back the encryption of pad rdra some further key material and some random things.

And then the new key that alice and bob generates is the hash of fa and fb this is a good time not to say that the establishment goes together with the dedication. Right? You cannot get a key from somebody that you have got with indicated. All right? That would be a very bad idea. I'm going to get key material from palace. Here in this process, others should really be authentic failure to be true. Otherwise, i'm gonna get keys from anyone. Right? Alice is indicated involved because of the random value. We have random value.

Creation is and the origin of indication Involved also indicated as if we affect the origin of indication creations. What do you think about the key management thing? Is this an example of key agreement or key transport? In other words, who has key control here? And is this it? And when we think about key confirmation, is this a protocol that has implicit key of indication or explicit key of indication? I give you a minute to think about that. Just me. What do you think about key confirmation? Is this a protocol with implicit or explicit? You have education is the new key that Alice and Bob agrees on. So this key idea is their existing key. They already have. They make me a new keypad. Is the new decay used anywhere in the protocol? No, right? This is implicit new authentication. The new key is not actually used to do anything. Whatever key control is this transport, or is this agreement? Does Alice have key control? Does Alice decide what the value of it is? Does Bob decide what the value of the key is? The answer is, none of them decides, right? Because it's a combination of what Alice is and a combination of what Bob is.

They both contribute to the key. That means none of them has key control. If we change that a little bit, we basically said there was no FA here. And the key is just that actually who would have key controlled out, who is deciding on the value of the key by itself as contribute anything to the keynote.

Now, right? This guy is the only person that decides on the value of the p is gold. Now it would be an example of e transport, because Bob is the singular party that determines the value of the e and that he is then said 2 hours for us. And it's your anything about country. Mhm. Next one, the establishment is in line, so this is with president party, right? We have eligible. They share already ttat with the trust of the party, and Bob shares, BT with the trust of the department and Bob sends random value to Alice, understands our own dragon value, Bob dragon value and identity involved with the trust of third party.

Trust the party makes a message that contains a message from Alice. Adam message for Paul, the message for Alice contains Alice's random value, the key material, the identity of Bob, some random text, it could be anything encrypted with pat the message involved is encrypted with PPT but that's rbf and the identity of you. Alice gets this message. She uses it. She takes this message before the default. At the same time, she also uses the new key that they agreed upon tad right?

To basically encrypt a new random number, a also regional random number. And they involved in the last slide response by encrypting these programs and value Alice's random value saving it to others. In this protocol, who is the thing you get it through? Who what type of key control do we have? And otherwise is this key agreement of the transport? And what level of key confirmation that you have implicit here in special or exquisite given that they are treating something about it. So, right. So what about authentication is Alice and dedicated to trust the third party? No, right? There's no data origin of indication of this message is bother dedicated to trust the party. No, right? Is there anything that goes involved to trust the party is rather than value? So we have some creation is to turn back to origin of education. It's just a third party is dedicated to Alice. Because against this man, Alice get this message could only have been encrypted with pat we trusted the party does. And Alice is a random number that she seems to trust it, but he's in talks with better or anything they get. It is trusted.

Third party is dedicated to ball. No, yes, right? Because even though trusted by the little directly involved, she says Alice, this message that Alice can send back to ball, right? And inside it is false notes interrupted with pdt which is something only transmitted, but you can do. So we have data origin and indication. We have freshness is Alice indicated the ball, because Alice makes this encryption with the new PAD and includes in it box knots. We have creations at the original indicator similarly walks in back to Alice with the new ead Alice is lost. So we have freshness at the origin of the indications involved is dedicated to Alice.

All right, so analyst is dedicated to ball box, is dedicated to Alice. Trusted party is dedicated to Alice trusted parties. Then you get involved. Why is it particularly important than trusted party? Is the thing you get into Alice involved? Because trust instead body is in the key, right? This value if is here is the key. So it would not be very good for Alice and Bob accepting keys from people that they have a lot of educated, right? That would be bad.

In terms of key management, is this an example of key transport or key agreement? There's Alice and I don't decide what the key would be, or Bob alone decides that the key would be one. Do they have no say in the matter? They don't decide, right? So trusted party chooses for them. Therefore, they don't have key control. Therefore, this is the agreement in terms of implicit or explicit the agreement. Does Alice and Bob? Does Alice absolutely know that Bob has the key or not? As well as Alice is trusting the process for the ccb using the key b uses the key, right? Similarly, Forbes sees others using the key. So not only that the protocol established the key to Alice involved. It also does something to ensure that Alice definitely know what has the key, what definitely no others have to keep.

All right, so there's explicit key of the education rather than Alice's keep involved and involves key to Alice. Right? So everybody think they have here is this model? Right? Alice has asked the key distribution center to give a key that she can talk to Bob with, but Bob is not online. So the key distribution center makes the basics for others. The message before we remember this protocol, then we also remember this one from the last lecture. The last lecture, we looked at this protocol from the perspective of the patient, but it is actually a key establishment protocol. And it is basically trying to do this. The biggest problem here, as we said last time, and linking to the fact that we said, we shouldn't take these from people. We haven't dedicated. It has a weakness because the process of the product is called the key. We have this message, but this message has no operations. S is never indicated to go. The weakness of this protocol is, therefore, that if I'm an attacker and I could observe this transaction between others involved at the trust of the party.

And then later on, let's say, many years from now, I managed to break this key. And I learned what tab is. But now this is not very useful to be, because Alice and Bob hasn't used that key for a very long time either. I can not go and try to get involved to reinstall that, because I can simply say, hey, Bob, I'm Alice. We are going to ask to trust the third party to give us a key. And now here is your key message, which is the one from 2 years ago. All right. And Bob will say this was made by the trusted third party because it's encrypted to BS that's right. And I am not going to use this pab and I'm gonna use this PA ab that indicated to Alice to make sure that Alice is real, but Alice has the key, not Alice as somebody else, but whoever is pretending to be, Alice has the right enough. So she can respond, involved, right? And basically she can give the right response involved. I just broke it because there's no creations in this protocol here. This is fixed by taking this RB right?

So basically, if we think if we try and sort of apply what was happened before? Fault is gonna say, like RB here. And this message that comes back here is going to include RB right? It's also gonna be over here, and it's gonna be saved by others today. So we have freshness. In that case, the reason that this protocol is actually was a very famous like academia is very famous protocol school. They need them and show their protocol. It was one of the very first protocols to try to do. He established, right? And it is also famous because the leaders throw their protocol was absorbed into windows 7,000 at the beginning of the century to be its ticket dropping.

So this is protocol, right? Not that this probability, they fix it by using a time stamp corporation. But you can see that many years later was exactly the same protocol just with the racial institution. So is still being used in facts. That is all I want to talk about today on the lecture. We can have right now, and then we can have the tutorial, and I will discuss the tutorial solutions with you at 4:30. Thank you. We are.