### Security\_week8\_tutorial-20241029\_16:32

说话人1 00:00  
I'm thinking about different design choices. Different files. We have not done the slide many times. To do an indication. We need two things, we need data or excellent indication, and we need freshness. In other words, do you think that alice, we need a message from alice that only alice convey? We have to ensure that alice has made that basis right now. If we have that, then we know that the person that we are talking to is us. If the message was made by a list that was awake, now it could be a weekly attack. If the message is looks new, but there's nothing there that only others can do, then we leave ourselves open to masquerade attack, right? So I have a question one, what is the issue with the following protocol? And how should we fix it in this protocol? We have others involved boxes to alice a random number, alice encrypt that random number and send it back before.

And then it is only with the issues still be there. Instead of interesting the message. Alice signed the message, right? So this is the reflection. In fact, we talked about right in that message over here. There is no identifier indicating the direction of this message. There should be ab here saying this is a message intended before, because that message is not there. If bob tries to indicate battery to check and see others, valerie can start this issue with bob at the same time, calculate the chief alice and he should have dedicated to her. Bob will then encrypt rb with ek that he shares with others. This message, it goes from bob to others. What he thinks is alice is the same message that alice would have returned to him to demonstrate that he is alice.

I'm not battery without calculating anything as the correct response and simply takes false response and holds it back to it. Right? And therefore, battery process. The part test is alice because the expression is rb and there's something that only alice you have done. Right? This does not work if we have signature. Right? I'm okay. So first of all, it would work. It wouldn't work if we could identify it, because then for the last message from bob to alice, there would be an a and for valerie to pass before the message would have to include ab right? That's why we have to identify it. For a signature. A lot of the cases when they do signature, they just would be identified as well. There's no problem doing that. But strictly speaking, the signature already implies some sort of direction that it means this is going from all to someone. So if somebody says bought his own signature, it looks a little bit funny. If we try to have a protocol with the signature and that we try to reflect it, the answer level gives the valerie is the signature by bob of rb but the message of valerie has to give bob is the signature by alice.

Once again, these two messages are not the same and valerie cannot just be big the final value. Two goals.

Next question, we talked about timestamps, we said timestamps in the actual time, or there can be logical concept and we talked about boxes and we said boxes are numbers that repeat for me once or happened only once, never repeats. And basically, it could be a random number, which is the best way of making it. But strictly speaking, a counter would also work as adults. If the counter discounts comes up, then obviously it's easy to know that it's nothing better.

In the following protocol, we've all seen the encryption of a guns, and alice is identified to alice. And alice is expected to decrypt it and we respond with n right? Would this protocol be happy with island loss?

In other words, can we use random number and a counter? Or can we only use a counter? Or can we only use and random thoughts? So the idea here is that alice is dedicated to bob, because it n is a value that is never reused. In other words, we have greatness. We don't really have a message. Only alice conveyed directly, like alice is something, anything assigned, anything or mapping anything. But the implication is that the only person that could decrypt this is alice. If alice can successfully decrypt it, she was obviously the acquisition of pk if the answer is back with the correct n then she proved it for a form that she asked. This is the thing I she could have done. And this creation is in this process, right? Would it work in this case, if we have a counter? A counter is, what is it counter predictable or unpredictable? If the nonsense is the counter, I can predict future value. Right? If i'm watching alice involved in the thing over there, and I see alice is back at ten, I see it back in 11 and I see it back in 12.

Now I know the next time. Alice will sit back at 13. So now I can jump in there. I can tell, hello, I am alice. Bob is going to send me something. I have no idea what it is. This is encrypted with alice more ski when I was going to send it back to 14, because that's a very good case and what it takes sponsorship. In other words, in this case, it would not be very good to have a counter. It really needs to be random. It needs to be something that an attacker cannot predict with this protocol to work properly. Ok question three, and is on a unilateral education protocol using for vertical one and five step in the encryption mechanism, and then put to a time stamp and map.

And then finally think about what the practical difference is between the time staff, using the timestamp with the encryption and the timestamps with a map, right?

For a we have a unilateral medication, so I alice needs to be thinking for we are using a time stamp in encryption, so it's gonna look like this. So alice is sending involved an encrypted message with pad with the time step, with the identifier of form. We have data oriented education from the encryption. We have. Creation is from the north, from the time stamp. So alice is dedicated to form. So what can bob do? Bob will take this message, bubble, decrypted. You'll see a phrase on stamp and you'll see identify. Right. Now it's basically like, then you can check the decrypt of time steps fresh. And he knows that the message was made using ead so we have said the origin of education. In the second one, when we use a time step and that others can send them back to evolve inside the mac or the inside the mac. The mac is done over the timestamp for alice and forth. I did. We should have data origin of indication from the back, and we should have einstein for freshness.

Now, the final question is basically asking you, is this protocol actually going to work? What is the practical difference between this protocol? A so on paper, if we do like the analysis and we say, who is the authority of the dedication? For instance, that's very good. Does this protocol actually work in practice? Can we actually use this in real life like it is here? No. Right. That is a good answer. Why? Because bob haven't actually checked that the timestamp is great, right? So over here, while he curves the message, he sees the time step. It's not possible to decrypt that, right? He can only verify that to verify the map qualified to redo the map on the time stamp. And for are you guys involved, so he knows what the identity is. But he doesn't know the constant value that others use.

So when we just look at it on paper, we can say alice has made a time check now. Bob knows exactly what the time is now. So bob can that's right. They realize he doesn't know, but he doesn't know how long the packet took to go from alice. Evolve could be a second, could be one pico second, right? One, the being to the - 12, right? They're very small, doesn't matter if it's 1 bit different, if this value is 1 bit different from the time step that alice in, then that is going to try. So for this protocol to work in practice, it must look like this. Alice was saying that time stamp explained x they send them back of the latex and the other part of dog.

Right now, bob can look at the time stamp because it's in plain textbook and say, hey, this plane takes that is 57 fresh, then takes this time stamp on his own identity b to calculate his full version of the map, and then matches it to the back diamonds. Simply speaking it, we have that example for the time stamp and signature in the lecture. It was a mutual one, right? With signatures, the same thing happened. Right? So remember that the signature is the hash of the content. Right? So to validate or to check the signature for also needs to know the exact value of the concept. The same thing happens with signatures. Right? If we want to sign tad we also need to put the ta outside. Sometimes let's say we directly cite ta this ta is shorter than the modulus. It is still not going to work for everything. It will work for rsa just remember, rsa has that special property that says, if you verify the signature, the original basis that you signed, it appears again, right?

But for those other signature algorithms, like dsa and the one basement of the law, the original message never appears again. You calculate the value of the value, and you make sure these two values are the same, but none of these values actually indicate the original message.

In other words, if we use signature, we also need to put the da outside, because that allows form to verify the signature or any signature scheme that you might use, or any method that you might use. It goes over the situation. Right? Question four, you are actually designed the education protocol for a web client to indicate servers. We want to build a system that indicate servers on the internet so that when I go there, I can verify that server is actually legitimate. It's the actual server that i've been visiting and lots of other server pertaining to be the server that I want to visit. You have to make the following design decisions. You have to decide whether it's better to use a five step or knots, and you have to decide whether it's better to use a symmetry, a or symmetric encryption.

In thinking about what is this use. You need to think about how many clients are there, how many servers are there? And how is their relationship who is going to talk to who? At the same time you need to think about what is the capability of your flight, what are they guaranteed to have? What might they not have? Right. So first thing we can think about should we use knots or client stamp? So when we talk about time stamps, we said it's very important for time stamps to work with both sides, have synchronized clock. They must have synchronized reliably synchronized clock, and ideally security synchronized clock. Right? So basically, this is not entirely guaranteed for every single quantity. If you're customer or if the person that owns the client, the pc the mobile phone is very tech savvy. Maybe they sit up. It would on service like synchronized to and on seller. It is often very nice. Some other people might be very careless, but the court might be 10 minutes wrong. It might be even their own day. No one does. There's no guarantee they don't have a single machine people actually carrying to check this.

All right. There's no real way for the server to verify. If we have a constant, it runs is probably going to be better. What about our keys? We said that symmetric encryption is good. So when we can use it, we should prefer to use it. But in this case, key management would be incredibly hard, right? We have billions of potential clients, and we have millions of potential servers that is a huge combination. So must every single client keep a shared symmetric key for every possible server that there ever been a visit? Right? That is probably highly unlikely, right? Same as often that we would probably say asymmetric mechanisms is the best year. All right. So basically, if the server can have a public private key pair and several pieces of privately secure, and it can give its public key to any client that wants to visited. And through that process, the server could be the main debate. Right? So what could this look like? So alice can seem to borrow a random loss as a challenge. Bob can sign that loans and send it back. Alice, all and basically, alice would be, et cetera. Bob would be a requirement. Okay? This works very nicely because now the senator has probably tried to keep there is a public key to the client.

The client can just put, they lost to the server. There's for server can sign it. The client at least confirmed the decision shares direct. And from that, the I think you get the server. In a few lectures, we'll talk about network security, and we look at pls pls is an asymmetric mechanism for the effective web servers. It doesn't work like this, but it also used a submission. And that is very interesting something for the server using the public key. And the fact that they show us that they can decrypt it. I think he gets a certain graph. They will talk about that more than you get. Right.

The very last question, we are asked to design an education protocol whereby clients will go on to online banking. You're asking these are for two banks. Both banks have to find to get the client a piece of secure hardware, and they can generate a response.

So basically the client has a program. This token can be a piece of hardware, which is increasingly becoming an APP, right? And that hardware or APP allows the client to generate some for the responses without them locking in the back. The difference is that 11 device only has the ability to generate the response. It doesn't have the ability to accept the input.

The second device actually allows for input to the system. Right? How do we design for device one? That's only the single button. If you press the button, then it generates a response. Should we use ignores our time stamp? We try to dedicate this hardware device, but there's no way for us to give it a loss, because there's no way to type anything into it. Right? So we pretty much need to use time step. Should we use asymmetric or symmetric pok so here we still have online application, but the online application is very different. Equation four. Question four was any client should be able to indicate any server. Right? So we said asymmetric propose the best. In this case, we have many clients, but we only have one server, which is the bank server. This is a much simpler place. Your bank already keeps details for all the clients anyway. So for the bank to just store as a matrix key for every client, would not really be a problem. And it's also possible to give that symmetric key to the client very easily, because the key is that you did inside the device that is given the device.

So key management is quite easy. It is feasible to use the matrix key. In this case, since the matrix is slightly easier to manage an isometric, in terms of the actual crypto, faster, shorter keys, that kind of thing if we can manage the management that would be preferable solutions. So we're gonna use symmetry mechanisms. Right? Then it will look something like this. So this is sort of the device that we envision. This was actually an rsa module. So the way they used to work is you just pressed one button. When you press the button, it gave you a response. You will press the button on the device. It will basically take the current file. And it might have been, I think the fire of the bag, it will encrypt everything, and it will give you a representative value of that encryption of that type of text that is reduced.

Okay? For question five b now, at the bank has a small, ten digit in your keypad. Those are backing increase for response generation. In this case, are we using indoors or timestamp? Not a device can actually accept input. It is possible to have a notes, use the dots, and then generate as a response. In terms of asymmetric and symmetric application is still pretty much the same. So we can use symmetric crypto. And then we can use it like this. So when we go to the bank's website, they might display as a Challenge. We will enter that Challenge into the device, and the device will use it in its response. Maybe do the back of RB and b and then the popular code to the facts, and then allows us, right? And then we sort of look at the advice and previously work on that. That is generally look like, as I said, most of these devices are not very little, but they still pretty much would in exactly the same way if you go back and out.

Yeah, II used to have one of these right back again, but not exactly differently.

Now, let's say, fine, open up. You have got some stuffing sometimes to pass with and then generate to the random number of the lobby. What do you want for us? Come back? Then you see. That is it for the tutorial. I will put the problem set solutions on the canvas. I will also let you know which ta market questions. So you can get answers if you have to be curious about, is it the and then I will serve prove the tutorial solution. And it does quite happen already put the notes prices on kind of. The one thing i've done is normally I only give the PDF for the slides, but I for lecture 56 and 7, because we have the protocols, sometimes some students said that the PDF doesn't really show very well when it's going on, because there's no animation. So I also put the PPT files there for you to work through. So you can see the date of measures, not yet. It's a little bit. So I have a good week, and then i'll see you next week.