### security\_week2\_tutorial1-20240910

说话人1 00:00  
At the moment, we have already done anything that because of the questions of seven, but easier, the tutorials are not stated to be entirely, very difficult, either. It's more just to put emphasis on the most important things you need to learn. Normally, when you probably did it, or what I try to do is maybe a couple of these core questions are emphasizing basic things I want you to know. It would be one very interesting question just to make you think a little bit more. Whereas this stage, we were only not hearing the data document, just to quickly do some very quick provisions about the important bits. We talked about the technology are great services and mechanisms. We know that red is the thing that mentioned. You got overall in our system, the thing that we want to prevent happening, or to take, if it happens, depending on what the rate is, then we have a security service, which is the control of the competition of the the goal that we have, the security that we want to provide. That's not even a race to create and make it less likely happen.

And then finally, can I have a mechanism, which is the thing that's actually implement the technical way we actually gonna implement, provide this service? So we look at lots of different services. The most famous one is confidentiality. So I have data. I don't want unauthorized people who see that data. So I don't want data disclosure to occur. The second one is integrity, rethinking. It's unauthorized by protection of data, availability, which is prevent unauthorized withholding of information. Then we have to do in patients in the of indication. I have a number of questions during the week, actually, about what the difference between the importance of indication is. Origin of indication is having a piece of data or message being able to know that alice made that message and that message has not been modified.

So in other words, we sort of so verify that the origin of the message was originally a long time ago happened. So whatever this piece of data, what was made by others and they still get on your point. Okay? Whereas in the education is maybe one step higher. That is the person I am currently talking to is alice. And we'll see later that when we discuss it in, the dimension is actually origin of indication plus something we call freshness. So I if i'm talking to someone and that someone gives me a message that was made by others, I can show that message must have been made.

Now. Other words, was it made a week ago. It was made now by the person i'm talking to, then I could say that attacks, there is an indication. This is origin of the indication of those months for verifying. We are to, rather than to say, this piece of data was made on access control that provides protection against unauthorized resources. Finally go to the bottom of mediation, remediation being I deny that something has happened, something has happened and I said it hasn't. I could either be I deny it ascending something or I deny it receding a message or else, okay. Right. And our services map onto various mechanisms, mechanisms to discussion more details. Probably week, weeks, our confidentiality index encryption, integrity. Imagine the signature availability to redundancy. It is indication of indication protocols, part of an indication of magnificent signature, standard mediation. It takes and carry access control, the axis control more.

The first question is just simple matrix, and then in some bits missing, and we need both in the blacks. So we have some sentences. We have to cover the empty list of friends. You mention other things. What are these things called? Which we're doing in the walls here? Mechanism. We have services, mechanism, algorithm. Great. Our service is confidentiality. Our mechanism is encryption. We can use variety. Encryption algorithms. A is this. What is the main threat to confidentiality? Disclosure gets better disclosure. All right? That one fixed. Second one we see in this map or h maps. Now this one is a little bit tricky. We'll talk a little more about that. You could say that this this is integrity. You could also say this is data origin of information.

Now it becomes a little bit of and difficulty in concept, because there are easy. I think origin of the education and integrity is similar. But you could argue the data argument indication is a smaller part of integrity.

Data argument indication is very specifically regulated message and very painful, and then it's been unmodified. Integrity is maybe a bigger picture. It relates to deleting things, it relates to modifying things, adding things completely. It also includes other services, a lot of mechanisms which are allowed to recover, for example, having a backup, something like that. Right? Actually, you can put the integrity or that origin information here. It would be okay. And what does it make for it to integrity or data, origin, information, I think, data modified, right? For the same second and they find it from under mediation. What is the mechanism for non remediation? Digital signature, and then create a repudiation as somebody to be potentially recipe design. Those are a lot of things. This one could possibly be bigger be and they are important. You put it again.

Okay. So the next one, we spoke about availability and availability as seen as the basic security service. What does the service do and give an example of the topic behavior based? So availability is there to ensure that a service that we are selling online is able to be available to our customer? Right? So our customers make a better service. Essentially, we got a one take that service away from them, and that might create it amazingly convinced if the part of service. So I spent briefly about analysis. It's about speaking said that it's quite needful criminals. They can make a lot of money for it. Right? It's actually quite common. Unfortunately, for a variety of reasons. So long ago, I had a student in the uk it was my last student. The master, either the project would be an england or a gambling company.

In the uki guess, many other places. They love to gamble enough to make bet on sports. Right? They want to make a course. They want to bet, especially on the tools. We are most of the sport events. The sport events are settled that afternoon. That's where the football game is. That's where the horse racing is. Most of the bits and they are in very big. So they're watching football these scores next door. Right? Who's gonna need a tough one? Who's gonna fall over the next? I don't know if they find everything right. If you're a baking company, that is your busiest day of the week, so your system goes down and your system is slow. The guy is not going to place an a to d but he's going to go to another guy in place to take it. He was telling me that they fight a lot of service attacks all the time coming from decorated them. Because if the back of the placement within, he's going to go to the underdog.

So every saturday when it comes, people have nothing is it is not a service again. Do you like make it slow for the clients? So the clients go to bed, so this is the damage more. This happens to me. Whereas finally popular, so i've never seen it as another service at that .. That's good. But it's an interesting. We don't want thing that is for these people, timing is actually very important. People wanna play a bit and what's gonna happen in the next minute. All right? And if they cannot do it, they didn't even have very good on it. So, okay, for a long time availability was not seen as a security service agreement. So when we look at that second set of services, the confidentiality, integrity, origin of education, modification, if I never let each not already there, that comes from a standard in the 1980s, even for cia the confidentiality, equity, and availability, in the early 90s that a was not availability, but it was implication.

But then people started thinking how availability is actually very important. So what do you think happened between the 1980s and today that everybody now suddenly thinks the credibility is really important? Why is availability become such an important security service? Whereas 50, 40 years ago, no one even worried about this. What do you think? What big technological advance do we have today that we did not have a 1980? Something that we use everyday? Online pay, online, only online pay that's online, right? The internet is a good, very good guess, right? Online or online anything, because in the 1980s they were learning today. Right? That way for the marketing anything online. Right? They were nothing. In fact, the way people go back, there was completely the opposite. It was when they just started making pc before that they had the mainframe architecture is a a lot of completely different. You have a very stupid machine on the desk and then talk to a big server somewhere, which is the size of the room. And then steve jobs and all these people came along and say, no, a few things can be different. I'm not going to be connected to anything. I'm going to have a little thing that sits only on my ass.

Now i'm going to do everything there. In fact, today we know that we went away from that game, but at the same time the internet started, and today we do anything or not. Right? You have to think every day I wouldn't go out to be different if there was no need today. I would be paid for things or emails or anything. Right? So life is not completely different, but 20 years ago, no one could proceed. Others would, right? So they will have them, and they were thinking about security. They were like, this is not important. What's availability? I'm gonna have everything on my pc that I hate. That was be able to disagree. Before what's the date with. Because of that, today, availability is very important because almost all services we use today are online. And if we are not able to go online, like as we know, it probably.

So, yeah. Question three, so we have a thing that we are looking for this newspaper as an item security adviser. And they have several problems, so they can use the name and possibly to the users. But I realize more and more people are basically sharing their password with other people or many people are reading. It would not have been possible at all.

The second problem they have, as they realize that somebody is trying to steal some of the subscriber payment information. Right? What can they do about that? And then the last one they say, some of the competitor, especially hacking, even change of the new stories, right? And then when people read the new story, there's a funny language. So there's some things that they don't want to say. And then you see customer somewhere along the line that verify what confidentiality is, what the invention is and what integrity is, but they don't exactly know how it applies. The business.

All right. In terms of an indication which one of these problems do you think it applies to these and then the password, the ceiling of the user information on the modification of the story? The user name and password, right? Because we're indicating the user, right? And they are basically failing to indicate the reserve, because lots of people who don't want to suddenly reading on this paper. Right? So that's how they think as a problem. This is a very common problem. If you have various movies treating website, for a long time, I just share my passport and use it there with someone else they can also watch. I've become stricter and stricter, much annoying me, but like not many extreme, right? Every time I try to watch basics anywhere, now I want maybe i'm going to my house that I have to do the issue of emails.

And so the difficulties I want to work instead of at home. Right? But I actually didn't tell us. So they get in front of faces, but it's actually a very, very hard problem to face. Right? Because as an example, industry, legitimate customer will watch or access your service different areas. So you cannot just say, I saw this guy's subscription most likely to use it at home, will only be good for that idea. So I might be somewhere else, right? So what do you do? I want my photo on the bus. All right. If I cannot leave it, then i'm not. So actually very, very difficult probably share to solve possible share. Okay. Confidentiality is that payment information or modification of data? Keeping kind of information a secret. So I come to the charity problem or is hard to find data on the charity program.

Potentiality is preventing the article thrice exposure, payment data. Right? You don't want to have the payment debt to see if anything else. Finally, we have integrity, right? So people want to find a few stories. Is it bigger people? Right? Next one, slightly different company is probably working for software data. The model of the company is that we will sell software online. People can download the software from our website that they install it locally and then run it. All right? So some of my customers are afraid that the software isn't really from the original developer that I might have modified it, so nowhere inside, and then I sell it today.

So what type of mechanism could I use? Or what kind of security services could I use to make sure that they trust me? Right? So that I didn't modify the data, right? Which reference means? Which security services do we have? That relate to data that belongs to somebody that's original? Data, integrity, good data already been indication of work. In this case, yes. So that's the origin of indication for a bigger improvement. Right? We need to be sure where it came from. Right? We can use a digital signature, or we can use it back. So what would happen is the original developer will sign, it will make it back, they'll give it to me and i'll put it online. If the user buys it, they can verify that signature of that back. They will know it is as good regional overweight.

In a way, I hope this looks like this already. Sometimes when you download the software for your PC and you try and store it, it won't do it, because your operating system says this does not come from a trusted data, because for drivers and some software, there are trusted developers by MAC trust developers by windows. Right? And they check the signatures on that pieces of software. If it's not a signature by somebody, they trust, they're gonna make it hard to reach school on the operators. After end of year, if it's a bigger that they really trust, it, might not even ask you for commission. I just explore it.

Anyway, so anyway, this is already a little bit powerful. The second one, this is the customer problem, so the customer downloads the software. And then later they tell me they want to refund because this Donald trend of the software this is. Okay. What security service can I implement here? So what is happening here? The customer is doing what is denied, right? You can do in order to get a ship, which one of origin of delivery. I guess I'm giving into the customer. I want a lot of repudiation to the research. You cannot let you tell me, sorry, I did not get the piece of salt.

So unfortunately, for us, there's not a really many mechanisms on the education of delivery or origin. We have digital signature, but delivery, we don't really have one. You can have the body at the station or the probation or loss. But in this case, maybe we can do it in the following way. I can basically have an encrypted product. I can send it to the client and then rather check some of it. Then the client will come back to me and confirm that the data was successful. An early day without giving some Oscar activate the software. So then you cannot come later and say the download failed because you already told me that the download was success. In a way, is not able to make it into this specific case, give us 100 deviation.

For the last few, pretty much straight from the slides, you're asked to prevent implementing the security mechanism, online chapters. It is happy to use standards, including solution. One reason we give you a boss, and that's why using existing standard opportunity, your own solution. So we know how to use standard. We can either see, again, it is already expanded that completely solve the problem. I can implement it and then ask specific nation or often defeat display compliance. Why is having somebody else check that I'm not correcting? Other one is just, you say, correctly, or I can look for for ideas and then implement. And then the last one, if I'm an engineer, and I just come up with my own solution, I'm trying to use standard.

My boss gives me some trouble for that. And why do we hire you? You need to design things. I think that I just gonna use a existing solution. Why is it exciting? You can tell me that it's going to save private money, right? Because the solution is already there. We also know that the solution is very good. Right? So that means our customer is gonna like it, and we are gonna make it good. All right? And then the visitors should be happy. Send, if the standard, as we discussed, is pretty much what most people think at the moment. Eason basis. This is a basic idea for that kind of solution. Eq system. Does it mean your system has to be the same as anything else? But for certain building loss of your system, it's really use. I think that are very step. So that is everything for the tutorial as of everything else. I will do the tutorial questions a lot. So you can also privacy. You should do it for real, in addition to thank you. And now to be recent, one p we get back to the Top. What's the matter? Why is wrong? A.