### Security\_week9\_lec02,lec 01没来-20241105

说话人1 00:00  
Yes. I just online with a web security. Probably the infrastructure has been very successful. Right? But the spider is not having this digital signature protection and legal protection for almost 30 years. The adoption for it in other areas is strangely slow. Right? And this would be because of the various reason. Right? I said this for public infrastructure, public encryption is not very well understood by all people, like, I think of tv public, but still be secure, like everybody can really understand symmetric encryption. You can go to anyone that's not typically expected that the violence secreted. You have a secret. We can do things in secret. They understand that. If I get to somebody and say, you give you to everyone, and we can put in secret, they go, I don't understand. Right? So it could be a tough issue there. Right? The other thing is just people get used to the way it works.

All right. If I come and suddenly say I was today even a log into the bank with the public, he said difficult. Instead of using that impossible, a lot of people would say, but I was happy with using that. I understood it. It was very well. Now you want to change it, right? You want to change. Right? So it's not really technical things, but if it is the business things or people things, right? There are many some technical issues, I hope, is that we have these laws. Most countries make this law. But sometimes the law is a little bit restrictive. So there might be a law that says, we trust digital signature, but we only trust digital signature diamond by public private key pairs that have been signed by a specific certificate authority.

For example, in a lot of countries in europe, it could be one single ca in a country that's approved by the government. If your document wasn't signed by a private key that corresponds to a certificate issued by that, cia it would not have legal protection. Right? Sometimes those c as are not very well known people want. Well, though, a big ca company that makes a really small government, ca right? So there could be some issues. Right? In a way, if it takes off, it would be quite peaceful like this. For my personal example, I only got this certificate a year ago. The only reason I did it is because in hong kong, I could not remove my driver's license with it. So previously what happened is that we need to fill in the paper form. I would need to go to a office. I would need to do like 6 or 7 hours and then got my paper form.

Now I can have app on my phone. I can upload everything online, and then I can digitally sign it with my certificate at my license come in, but ii saved my day. Okay, that's the only reason I get it. So maybe if we get more applications like that, people also start and copy the statement. Right? But we made. So to end with, we can just talk about a couple of examples of the management. The management is often boring. I think there's nothing really exciting happens. So the drivers taking the values and lead them to people. But as I said at the beginning of this lecture, it's incredibly important. We can have all these fancy crypto algorithms and signatures and encryption and fancy systems. But if we don't ensure that our keys are actually secure, and our key is going to the people that needed, all of these systems do not work. Right? So we will look at one practical example, despite an interesting event problem.

Then we'll look at one example where the management was quite a big problem or something quite fancy happened in the community, but it was essentially the management. So these days we all have electronic passport. Passport has always been machine readable. So by machine readable, everybody's possible has this optical recognition strip at the bottom if it was always machine readable. All right. So id cards and passports, most of the security came from physical protection. Right? So physical protection and physical security of documents is itself very interesting, right? There's lots of interesting things that people can do. You have holograms, you have special teams that you have micro printing, all sorts of things, micro printing is. Sometimes if you go look on the high magnification, if you have pictures on id documents, if you magnify them a lot, you actually realize that they are not drawn, but they're actually made up of printed words. Right?

So the idea is that the person is legitimately issue of card. Their predator is better than the guideline, the card. That thats essentially the problem that thats the answer. If I have a better printer than different smaller things, more accurate things with more colors, then I can make a document that is not portable. Right? But that is only useful with so long. One of the earlier things that happened was that people have always been worried about people forging money. Right? And for a long time, you needed quite spatial technology for the money. And in some case, and then some cases, then photocopiers became so good, then you can basically photocopy money and make possible contract for the book. Right? That's why a lot of commercial photocopy area, you actually trying to copy money. It will refuse to do.

So actually recognize that you put the money and it will just put you out of black page and say now I won't copy this. Some of the photocopies actually have that either. Right? Because you can make pretty good photoshop. So what they said was for a passport, which is the present most important digital document, we can't only rely on physical security measures anymore. We have to make a copy of the photo page, keep a copy of that information on a chip in the passport, and the government will sign that data. So the idea was that every single government in the world will have a public private key pair. It will share the public key with all the other countries in the world and they will sign my passport. So if I cattle, when I reach the border, I give my passport, the passport goes on to the machine. The machine reads it, and displays my information and verifies my country's signature of that information.

Now, my passport essentially becomes unforeseeable, because before people could always mess around with funny things, but they cannot forge that signature.

If the officer who took my photo page and it shows it in data, and then it reads the data out of the chip and they are different. They know that something weird is going on. Right? So very good idea, right? Immediately people complain, right? Because people were like, okay, but what do you mean? This data is now readable out of my passport and who is going to be able to read it? Because if we put it on a contactless chip, which it was immensely, it means I can have it in my pocket. Somebody can walk by and read everything often. Right? I i'm not happy with it because this is my personal document. There were some people like youtube doing very crazy things. There was one guy trying to make an argument that you cannot go to form that will only go home for the specific person will find. Does he may like sort of a faint wall?

And then with the rfidv there and with the physical passes, sort of like states that it's alice, and then it would like little some power. But this became very popular saying that we didn't want this. So what are you going to do? So whereas the signature was easy to verify, because we could just share public key with everyone. Right? This is not a problem. So they said, how do we do access on call for this car? That either we actually share another key that allows the car to indicate the border control agent or the reader. Only after it just indicated the reader is a download of the data. So if we wanted to do this with public key information, it made that the passport itself we have to store public key certificates for every single country. It would have to be put on there when the passport gets issued, but the passport gets issued to last for 10 years. And one of the countries, probably the certificate expires in a shorter period of time and time, which it's more likely anything to be better than 6 months.

So I couldn't do that. So they said the only way to do this is to use symmetric key cryptography. Right? And they said, how can we make the symmetric key? If I use my password, I give it to the person at the border. So they said, okay, by giving it to someone, I consent for them to read it. I agree that there are a lot to read it. The easiest way to do this is for that person to read all the information on my photo page.

And then from that photo page to derive the symmetric shared key. And then that should be shared, symmetric key could be used to read the data of the chip. This work because if I gave my part to the border agent and they scanned it, they could make the key. But if i'm just walking down the street and somebody's trying to read it in my pocket, they don't know my personal information. So they cannot read my password. If they knew my personal information already, they wouldn't need to read my part. So this is quite a good solution. The only problem with this solution was that they got their calculation wrong for how strong that he was going to be. So the sentence is that this uses is it needs a 56 bit key. The way they derive the key is from the serial number of the passport, the birthday, and the expiry date will become.

So what do you possible? But when they calculated it and they said the total number of possible dates you can have is from the year zero to the year 9,999 from month 1 to 12, from day 1 to day 1. So we multiply all that together and we do it for the serial number of the birthday and the expiry date. We have a number equivalent to certificates, but then people pointed out to them that no one that has a possible today, we have a birthday year zero. Right? Most people who alive today is probably born in the last 90 years, hundred years. Certainly if we look at the expiry date has to be somewhere in the next 8 years. We don't have the full range of pay. We only have this very small rate of pay. And they also found that a lot of governments would issue serial numbers that are sequential.

So in other words, I can get my password today. My number is 10, and that means the person tomorrow gets 12 and 13. We never go back and find. So actually, the key string only about 20 bits, maybe 25 bits, which was very bad. Right? The people who better if you guess and then trying to reinforce it for the key and read it in your pocket and maybe another no. So that can change. And they said we can't change the list and expiry date, but we'll change it so that everybody that has a passport should have an elephant in theory. Random id value, what they call for the zero number of impossible.

So then we add the extra letters in. We also don't have it to be separation. Right? So interesting, real world key management. Right? The next one is more impressive in a way. There's basically was a piece of nowhere. I think it was around 2010 and it was called stocks in it. And stocks in is still a big thing. The reason stocks in it is still a big thing is because stocks in for its time was probably the most advanced piece of nowhere that anyone had seen. It did some things that were quite interesting. And I think at the end of the decision on it was that it wasn't really just a general piece of nowhere, but it was really made to be opened like aaa cyber with. All right. And people have not really seen this before. So stock center is interesting because it spread through windows, and it spreads through with us using what is referred to as 0 day exploits. So zero day exploits in itself is very powerful, because that's why that no one has seen before.

So we spoke a long time ago and makes you wonder about people getting hacked normally when they get hacked with no techniques. And it was just that they're a bit lazy, and they should have known about it, but they were not on top of it, and they were hacked. Zero that exploits are ones where no one has seen it. It's basically a probability that is used for the very first one. If you find zero, the exploits actually take a lot of skill, because there's people everywhere continuously looking for exploits, and actually finding some that no one else has ever found is really hard, most early valuable skill. Right? The practice people try to avoid this by having five hunting values. If you can find it zero that I exploit, you can legally sell it to some company and then you get award rather very nice and discouraging from using active.

You can basically sell it today and say, I disclose that I found this issue and give you some reward. This is the way people do the zero effects. There is no other way to deal with it, something that people have never seen. Right. The other interesting thing was that it tried not ready to reach what we think about as conventional, secure infrastructure, IP infrastructure, but it was trying to get into very specific industrial control system. So we use internet and we use internet, we use WiFi, because we watch videos online, and we makes a comment to buy stuff. But in factories, they use different kinds of internet, different kinds of IP things that are designed to be super reliable, because if you are in a factory doing manufacturing or process control, if I'm watching video and my internet goes on for 1 second, and my video is also 1 second, and then we offer that's okay.

In factory, if that happens, factory might blow up or product completely broken. So they have special internet about special communication protocol, factory, automation. And they have special computers called probability controllers for that. Another interesting thing is that stocks are trying to get onto these things, success with the work. So we'll talk about the next weeks and try to spread, and nobody will spread indiscriminate. They just try to go everywhere as much as they have. In this case, foxy doesn't work was a bit strange because there's some countries that it wasn't interested in at all. Some other countries are sort of straight by accident, which is the green ones. And some countries, it seems specifically very interested in specifically the red one here, which is Iran, right? I don't know why I was interested in Indonesia, but that might just be like mistake.

But basically, I wanted to go to Iran. It was its main purpose to go there. After a while, people brought the mail where they did the analysis on it, and actually found out the third thing that was interested in about, starting from the zero day to the industrial control system. It was made to get into an air gap system.

So air gap systems are systems that are so secure that they don't actually connect to the internet. So literally, there's a gap that they're not connected to anything. Right? Because what I wanted to do was it wanted to get onto USB drives. That's all USB drive. It would transfer to them, and it would hope that somebody would one day would get onto enough. Usb drives that somebody would take it and plug it in the system that it was really positive. Right? What I realized was that thing that it was pocketing was made here in Richmond thought in Iran. That is what it was looking for. That place is not connected to the internet. So they try to infect enough p CS at home.

So one day that somebody working there would take a file home, some work at home, his or her USB drive would get infected. They would take it back to work the following day. They would plug it in. They wouldn't say that system which it then eventually did. Around this time, they realized that the ritual fund has gone offline, because the programmable logic controllers, no function.

The story does is that what stocks needed was it has cooling turbines. What I basically did was it started spitting up these turbines to go as fast as they could possibly could. And then they suddenly put on the emergency break to stop there. And the force was so great that these turbines actually broke. And as if he had reported, this took this 441. So therefore, it is not very popular to talk about even today. So I think since then, no one has even seen something like this paper again, right? No one knows who made it where it comes from. You may be made some cases, but no one knows what you are. Right? Either, how is this a key management problem? Despite all these fancy things that happened at the core of stocks in the validity to get on, the USB drives the ability to spread itself to other systems, the ability to infect the programmable logic controllers came from the fact that it could be sort itself as a device driver.

Right? Device drivers are quite trusted hardware because it operates quite low down in your operating system. Right? It gained access to a lot of low level hardware. Everybody that makes hardware for p CS, commercial hardware for p CS are considered to be trusted softly developer. And they signed the device drivers. And their public key is already cached within your operating system. If you want to install a new driver, the operating system will verify the signature of that fiber and it's from a developed presence of node. People are fears to be installed. I don't know if they try to install some funny hardware on your PC and then it tells you this is from an unprocessed inventor. We are going to do it in a way that it's quite strict. You can eventually force it, but you actually have to boot into safe mode and disable a lot of things to be able to otherwise avoid.

I did stocks in, do it, somehow ever made stocks in it, broke into two companies. The one that's real f the other one was today micron and dial micron and real tick. Make hardware like real tech is known for motherboards, sound cards, that kind of thing, lots of almost every single model, or you can buy commercial, you have to build a stuff, very important stuff. We're basically on board graphic art, on board sound modules, audio, that kind of thing. And basically stocks, it was signed with their private key. Right? When people realize this and the very sign is a very important ca all right. Various I realize this and revoke a certificate, Saxon immediately reverted to a stake in well known companies. Priority, right? Which means whoever did this also managed to physically go to these companies, hack them, get hold of the private, which is probably the biggest issue, right? If you are at that level of trusted development, your company should probably take better care of the company.

It's final down the fancy things that we follow on the core part of violence work with. This is the faculty, is that two companies couldn't really tracked on where the private vehicle. Okay. That's all I want to say this week. So start with the punishment next week. We'll start talking about computer security for one lecture, and then we'll have 2 weeks on network security. And then we have our recent thoughts. Actually, we've done 9 weeks of 30 what's about being done? Okay, so the other thing is that I don't know if you know that the university is currently collecting together Information for exams. So I hope that you will have some Information on when the exam will be in the coming few weeks.

Okay. Ideally, I think I will try to have the exam exactly the same time as you do yourself. I think that's the way the others are from. So that exam has not been finalized by them. So I think we'll hear about that one next week. They've got one campus will make decisions about exams. See you after that. But if I know, you will know, I will tell you. Right. But either usually the city one is in the evening, because all the master courses there are in the evening. So it will probably be add as well, too. But I don't know exactly which day somewhere from the 16 to twenty, thirty. December, we'll talk about that, which I know. Thank you. That's all for the lecture. And you're sticking around for the tutorial of discussing tutorial solutions. At part possible. Thank you.