### security\_week2\_1-20240910

说话人1 00:00  
I think I could start just a case study or reading. It's cool about. She was so neat. It's a nice story, even though it's a much older story, it's for more than 10 years ago enough. But it gives us some insight into even our companies see security breaches today, because they haven't really changed that much. And it's also nice because it mentions a lot of the things that happens when I talked about in this class just to give a brief overview if you haven't read it. So in 2011, so need something quite a big pack on the plane station network. And at the time they had about 77 million users baker stolen. So 77 million is, unfortunately, not about these days. This was not really rank anywhere. The biggest data breaches we've had since. I believe the biggest one has come for, it was about 11 billion. Pieces of data is going backward. Yahoo has a very large one about 3 billion. So in that context, 77 million is big, but at the time, this was much larger than anything that had happened before.

Okay? So essentially, they notice that the servers were recruiting, and they didn't know why they look into it. They realized they could act and somebody took some of the data, so they took some of the customers personal details, in addition to get it prior information. So at the time and school today was earlier already, most countries in the world has data protection law. So if you're a company and you suffer a significant data loss, you need to report it to someone.

So I need to report to that to the us government or to the different states they were operating in. Everybody was very concerned, and they actually had to go in front of the us congress to explain what happened. What they then said was that they were basically attacked by a super advanced adversary. They were subject to a very advanced attack. They couldn't have done anything about it. This is very common. So in the article, it actually refers to the doctrine of defense. Then star wars, star wars is got paid. There is a different right star wars. The idea that everybody that hacks us is super powerful like a big movie that they have so much steel. There's so much resources. Even if we have tried, we would not have been able to take the game. Right? In some cases that is true. But unfortunately, in most cases, it is not and it definitely wasn't the case in the case of sony. Right? Later on, and that various other people testifying, eventually, an activist group to get also took responsibility for this act.

At the time, no one really knew why the attack happened, because none of the credit card information on data that was stolen, obviously got used in any fraud, right? Wrong. Subsequently, it came out that they were basically hacked by activists, because activists were unhappy. Then they were prosecuting somebody that act the digital rights management for playstation, like people copy games, play games that they haven't been.

So anyway, the case against this guy, he was quite a famous actor, and his face is unhappy. So they're acting concerned in popular bench. What they said is that they actually use very simple attack, simple sql injection. And everybody that's read a little bit about security and hacking no sqr injection at the same time.

When other people look at this system, they say, actually, there was no big attack. Here. The attack was very simple. The issue was that sony did not protect this system properly. They have very poor operational security. They were not catching anything on time, and they didn't really have strong security management. The biggest thing that happened was that they hadn't, they had an apache web server. It had no vulnerabilities. So if you go online, if you're running large software systems, even if you just write your pc that you have to update every few weeks, right? It's going to tell you what you need to restart. Not often. They haven't really done that. Right? They were known vulnerabilities in the version of the web server. They were running. They never wanted to fix it, even though it was a well known problem, and the hackers use that to hack it. So that is not really the attacker was so powerful. We do nothing, even though the attacker had skill, they didn't really need. Because it was said, easy to have it.

So many people actually disputed the defense and say you just happen to be really bad. The other reason that came out is that if you have payment data and you have personal information, why was your data not encrypted? Because that should be the obvious thing to do.

All right? And the outcome of this was that they actually mentioned that only encrypting, their data would have doubled the it requirement. Just in cripple that data, then having to re encrypt and encrypt as people were logging in as people were using, it would have doubled the need for the ip infrastructure which would have doubled their cost. So they just took a decision not to incur.

So solving the problem would have been very easy, but they choose not to do so because it is expensive. Apart from that, they left their system, open the very basic attack. And that's sort of a lesson to learn from this. We saw last week, we talked about different labels on the attacker. At the end, we did mention these people that are extremely skillful, right? But the chance that they go after you is probably very low. The biggest thing that happens is if you are managing the security for a company, it's about doing the basics, right? And that will probably prevent most of the attacks. Right? We had some questions that we posted for this. So we said is a security vulnerability, almost related to technical aspects of the target is, in fact, always technical in nature.

And in this article, find examples of technical and non technical and weakness is exploited by the effort. Right? In this article, it actually mentions a number of different things. It mentions denial of service, spr injection. There was very good viable configuration, and they were using the website. We would know probability those are your technical issues. It also mentioned fishing, so fishing will talk about later in the course. A fishing is, once again, not a technical act, more of a social engineering role. Like people will try to contact you, send you email, try to fool you into giving you bad personal information. Right? What type of adversaries are mentioned in the articles? Remember, in the course people provide more people, board insiders, criminals, sort of advanced. This is great, and then finally activist.

So in this case, we pretty much activists, economist and policy is famous activist or hacker groups that are mentioned in this article, which security services and associate mechanism is said to be capable of making this data, which is serious. Do you remember the concept of service and mechanism service being that the goal that we have mechanism being the way that we want to implement it? Security service we needed, in this case, was confidentiality. We had a disclosure of information. Service is supposed to investigate that confidentiality, and we couldn't provided with encryption. But as I said, they didn't do it, in this case, because they did the business decision. Let's say it's going to cost money, and they paid too much bigger price for it in the end. Right? Either the real issue was more operational, whoever was in charge of the security systems, made basic errors, like not updating things, not keeping on top of what the current vulnerabilities. It's obvious need for certainly that quite a bad reputation.

So apart from this one, which is quite famous, but actually several years later had even a bigger pack. Right? So hopefully well better than anything from the same stuff that he said no. Right? Subsequently, somebody had to do them again. And so all the underneath movies and all the emails from the executives and everything probably it's quite embarrassing at the time, right? So one additional question we can think about that I didn't give. We said that security e commerce is very important. I think we talk about one remediation, online contracting. Right? So why do we think security is important when we do things online and who is harmed by the security of my public damage? The first one is maybe easy to answer. Everything we do is now online. Right? We are more connected to each other than we ever were. So that is good because it allows us to do lots of nice things, but it is so bad because we connected to every single bad person in the world.

All right. Back when we had a physical store in a little town somewhere, the amount of people who want to rob me, you want to break into my store is very little. They have to be physically located. There are people can steal from you wherever they are located in the world, because we all connected a lot.

The second one comes to who actually uses money when we have security issues. So there's actually three people, right? Or three entities. First of all, if I suffer embarrassing security incident, my own business is going to lose. Maybe we lose some money, but it's often that it's not like our money gets directly stolen unless we are subject to some kind of role. If so many skills are customer data, their payment card, obviously we are not gonna suffer really. Financial loss. The biggest issue that we're gonna suffer is reputational loss. Right? And sometimes that is even more important than the money, because money is actual money, my reputation is money in the future. If we don't look after the system properly and we get back, our customers will need in the future. We don't get new customers. They're like, why do we want to deal with these people? Because these people are gonna use our information. These people are not trustworthy. Their systems are concerned.

Therefore, it's important to do things, right? The other person that we are having is our customer, right? Our customer, if we lose the information, will be subject to follow up fraud. Right? You have to think about how we deal with lots of institutions today. If I follow the bank, the bank asks me, what is your first line of your address? What is your birthday? Can you call me the last 4 pages of your phone number? Can you call me your bank account number? And that is used to authenticate people in everyday transaction? If I lose that information, as I asked the customer that information when they sign up, how many websites are you for your birthday, for your phone number, for your address? Right? If they get hacked and somebody doesn't make this database and sells it online somewhere, then people are going to phone you up and say, hey, i'm the bank.

I'll prove to you that I was back because I know where you live and I know what your phone number is, then it becomes very hard for your customer to discern that guy phoning them is competition, right? If I lose this information, my customer might be subject to follow on floor in addition to loss of privacy.

And basically people being quite keen, get private data. The third one and last one may be the toughest business. Is it separate laws is other business? Right? Once again, they might want to do business with us because we have let them down, right? Maybe something we have done wrong open some portal for attackers to attack him. Okay. Recently I think there was a good example of this. It was something with booking dot com. So looking up from apparently as a portal that gets downloaded by hotels, to be able to verify bookings made it themselves.

And then therefore, some hotels of courses actually follow the hotel, managed to fool the people who work there into giving them access to the system. And then from there, they got direct access to the booking of home portal. Once they were in the booking dot com portal, they started attacking individual customers. This is a very complex chain, iphone up a chain. The hotel chain doesn't do good operational security manages to use the lobbying details that looking at home server. Attackers go into the booking dot com server doesn't attack booking dot com, but extract information to attack customer, because then what happened is they see the customer as a booking in 2 weeks from now for a nice hotel. They thrown up the customer and they say I am from booking dot com, I see that you have a booking at this hotel 2 weeks from now. However we never received your payment. We are not going to cancel your booking. The customer doesn't know what's going on, because the person phoning him knows about this routine. And they know all his personal detail.

So it's very difficult for the customer to think while the person calling me is not actually here, then the person will say you need to pay again because we did not get your own payment, Pay money into this bank account. This time it gets a little bit suspicious because looking the company not ask me for the money to back it up. Okay, but there are lots of people deposit money if you drive a car lose money. Right? And this is like a chain of different people whose security is not really strong. So you could say is the hotel should not lose the login. You can say that in the country probably have stronger log in their own business customer, but you can see how this all lives together. Whenever we need a bit of data, they can only for the things. Additionally, if we lose credit card number and somebody else then comes and does fraud with it, goes to a store, buys an item, right? And later, that admission will give the item to the customer which is discover. Right? And later the real owner of the car will go to the bank and say I did not like this. Okay?

Then the bank says we kill this payment. The customer gets the money back if they're lucky, if the bank believes them, and then they mentioned uses the money because the bank journey never loses money. It's called a charge back.

So I I if I put something on a credit card, if I see this as a species transaction, I have the option of finding out it again. And then even if the merchants already been with the service, the merchants, right? All this information looks a little bit like not really valuable. What can we do with it? But people are actually very smart and exploiting this information. So everything is connected. Data is used everywhere in different ways. Once we even do simple data like birthday for accurate phone number, it opens up in entirely new window or floor. Great. So I will put those slides alive. So you don't have to worry about it, ok so that's good. Just before we start with some announcement. So today we start with the tutorial. I think one tutorial is gonna be in 415. And the other tutorial at 5 o'clock was gonna be in 417. When we got email to say, 417 broken at the moment. So both tutorials will be in ac 5415. Okay? Second thing last week, I said, i'm gonna try and figure out how to report the lecture, but I managed to record lawsuits, nature, and teams, but I cannot do that to you because as it turns out, the university's configuration allows you to download, it's not allowed to do.

I've spoken to it offers. They have another way that this is gonna happen, but they cannot set it up for today. So from next week, hopefully, I will be making recording of all the lecture, and you'll be receiving something to do that. And they perspective for your own reference. And then for next week class to applause, because we have the public holiday before the festival. So just remember that the next class is on the 24 september. And then as for the university timetable, the makeup class is exactly the same time. The same classroom on the 29th. Starting off. Let's just think about we did last week. We talked about basic terminology of information, security. We have talked about the basic idea of threats, things that be positive were wrong, services that we want to implement to prevent the threat from happening mechanisms, the actual ways of providing and implementing the service and algorithms being the bottom building blocks of each one mechanisms.

We can talk a little bit about where we can find good mechanisms and algorithms and confirmations. And we talked about standards with a little bit of view on security standards where they come from and how they get greater. And some positive and negative aspects of that. We talked a little bit about different senate bodies. We talked about internet company standards in today's lecture, which is also the next lecture, because the state of lecture slides go over 2 weeks, right? We're gonna talk about confidentiality. And specifically, we're gonna talk about symmetric key encryption, right? This covers the course, intended learning, part two five technology that impacts systems and security mechanism. This lecture is slightly structured in two parts. The first one is sort of an introduction to security and encryption, because for a long time, whenever we talked about information, security and topography, it was pretty much making little code and cyphers. This predominantly the encryption, we sort of taking a historical view, and also later about exactly what type of viewpoints we trying to get across.

The second part is then actually getting into state of the art and modern and symmetric ok essentially, cryptography or proposed has fascinated people for many years.

So it's actually very, very long. All right, more than 2,000 years. Okay, anthropology has always been the art of making secret codes, basically code making with cryptanalysis being code breaking. Right? So in other words, security existed entirely based on the property photography with making little puzzles that you could use to hide information if you have any kind of code. And at the same time, a lot of other people working on how we break these codes. Sometimes could be quite simple, sometimes could be quite complex, right?

We just look at the simple one. Can you decipher this code here? Where is this? The idea? It's cryptography. Right? So this is just somebody jumping up the letters of the word. Right? This is drawn into what is we know today as crypto, modern photography is that we have modification everything, patient protocol, we have identification protocols, we have your knowledge, we have exactly commitment lots of other things. Right? So this is not necessarily a crypto course. There are some people that are very interested only in the crypto, in a mathematical way, make it be underlying hope. You will do a little bit off, but you have covered everything. If you are really interested in looking into the history of photography or even more than like photography, there are some good books, like a public evolution higher. The angles of the pipe of probably introduction towards person. I think the angles of the pipes probably great. It's actually free to be, I think it's part of the books. I and that one could be, he wanted for the about this.

So why don't we go back in time a little bit? So simon singh wrote a very interesting book and called the code book that covers the history of photography in the idea that for a very long time, it's basically been the circle. I find a good way to hide my information. You find a way of breaking that way. I didn't find a better way. You find a better way of breaking it. I need to improve the factor improves. The predictor improves this continual arms race between people trying to protect data and people trying to steal their data. Right? And we're gonna go from the beginning. We're gonna see sort of what the very first cycle was, and maybe to see the people program how people talk about changing it, and then how people broke it again. And this will give us a natural preparation if you want to die.

The first thing that we need to discuss is what we mean by symmetric cryptography. We have two models for encryption. The one is symmetric, and the other one is asymmetric. Discuss later. So in symmetric cryptography, we have two parties. So we have alice. We have got and then the two participants, and they want to send message to each other, and they want to attract, or they want to protect the message against external attacker. Right? In a symmetric system, alice and bob have the same secret. So they share a secret that only they know. So alice knows something, and bob knows exactly the same thing. We were referred to that as the key. So alice has a secret key, all has a secret key. They do not share it with anyone else. And they can use that secret key to send each other data.

So alice is gonna use that key to encrypt our information. Information that we can just read is called plain text. You're encrypted, and that will give us cited text. Bob will then take the same key that alice has used with. Bob also knows that he the encrypt the size of the text and that should give you the plane takes back anyone else in the system. They are looking to either find the plain text. Or ideally, what they're looking for is the key, because if they can find the key, then they can decrypt any message, right? Between other support, right? In a sense, the secure system is one where alice and bob keeps the secret key. He did from everybody else. And if they send socket takes to each other, an attacker can neither see what they say. Of the cycle case. Panels are not recovered. But the concept of symmetric means same on each side, and alice above has the same key.

Okay? When we're dealing with the analysis of these persistence, there are some good basic assumptions to make. The first one is that the entire system is known with a factor. And the only secret that there is the key. So this is actually a very well done concept, name, cook off principles. So this guy cook off, came along and said, if you want to build secure systems, you cannot do it on the basis that people don't know what you are doing. Because eventually this will fight. So in modern times, people call this security through obscurity. My system is secure, and no one has hacked me, because no one has figured out how it works yet. Unfortunately, figuring out how it works, if you try really hard is not that difficult. People can reverse engineer how things work quite easy. So if i'm using a really bad cipher, but i'm sending data, no one's managing the encrypted period on the fact that they don't know what cipher are using. It's not a good idea, because eventually they figure out how it works.

And then once they figure out how it works, then i'm sitting with a bad system, a bad algorithm that is then easily practical. Right? The idea is that even if we tell an attacker of everything about our system, except for the secret key helper, alice involved, and our system is secure based on that, our system is well designed and is very strong.

So first example of symmetric encryption was done by julius caesar. It was called the caesar cipher. It's a special case of the substitution cipher. It was used to encrypt simple, short messages. What is obvious right for their own empire? If you just look at these words, I don't think you could really guess what they are. And here we had that simple photography thing that was a good job. If you look very quickly at these, you cannot be the pc what they are, right? Both of these are encrypted with the caesar stock. What a caesar cipher was is they use the roman alphabet, which is built the alphabet we use for a lot of languages today, and they substitute the plane takes later for a soccer taste data.

And in the case of the most classic judaism to suffer the shift in the value between the plaintiffs alphabet and the sophistics alphabet is 3 ..

You can see that a moves three positions on 123, so it maps to ad then the b moves 123 maps to e your c is an, a to b is ag so the cipher takes. Alphabet is also an alphabet in order when all the letters has moved over by few conditions.

So very simple, stop it. This was the first case. Cryptography, either we encrypt and decrypt, we basically write down our substitution table first for our alphabet substitution table. We can write down the plain text that we want to use. And then we can simply map, we can say okrh is going to map to ak then we're gonna have an e it's gonna map to an h we can have an l and map to o another o and map to r and then you can do that. Everyone you e be more. You get the idea, right? We simply write down a substitution table, and we can map cross. And to basically decrypt, we will do the opposite. Now there is recipient will get the message. And they will use the same substitution table, the same ship with alphabet, but they will go in reverse. They can go for k h h goes to e they can go and go to the ls and are so quite simple.

Okay? I just want you may be talking about you. Can talk a little bit. I want you to maybe just try it. I'll give you a couple of minutes. You can try to decrypt message one and message two, right? That is encrypted with ac to cipher, shift three and give you about 5 minutes 50. Answer. Your answer. Anyone have an answer for one? You everyone you do the answer for one is a four score at 7 years ago. So four score is a very old, ancient.

It is good for 80. I want you to anymore. So it's 87 years ago. The second answer is 54 square 5, the one for the basic student. So if you manage to get that good, you quite part of it. It's a good. Basically, you think that part substitution side of the worse concept, very easy to understand mapping one single word to one single another word. Okay, so the weakness of the Caesar cipher is obviously that we only have 25 different. We call it keys. Because if we're doing the encryption, we always have to shift the alphabet. And the alphabet can only really shift 25 twice. After that, it becomes the same as shifting it by one or by two.

Again. If I figured out how it worked, it would be very easy for me just to try all possible combinations to see what the message is. Right? So people moved on very quickly from what Caesar had, which was just simply shifting the alphabet towards making it basically a Complete permutation of Alpha ok okay? So there were variety ways of doing this, right? So one way that people could do this, which is also a good way that people say that we can create password is to have some kind of pass phrase or quote. Thats easy to remember.

In this case, for example, we have pure mathematics is in its work in a way the poetry of logical ideas is a good part of Einstein. And we can basically generate the substitution table by just taking the first get there in each case and stripping out the repeating letters. What we can do is we can have AA sentence. This is the first time that the key. First we write down the key, then the first u the first r the first e the first m ath and then we said, but there's an e here, but we had a key before. We just gonna ignore it. Also, at the end before a we also had a key before, so we ignore it.

Now we have an I I is new c is new, s is new. I already had s already, the in is u these three are the same as before. The w is new. Why is you are getting sort of to the stage? We get most things before I would have l and GD then we take the second line and we write them down in order, right? And that has become the first part of this substitution of it. All right. So we end up with the substitution out of it. And then basically, we can just filling the risk. Maybe you don't have. That is maybe this guy is the reverse order of all the makers. We did not have that. Obviously, this random communication of the alphabet as much less likely to guess as a ceases offer would be. Okay. So it's very unpredictable.

So now we move from basically just a a shift of the alphabet towards a completely rather for the patient of it. The idea of a substitution cipher in contrast with shifts I heard is that our entire alphabet is random, or here is random to somebody else. The big family of cipher that works in this way where we substitute one letter for another letter is substitution.

The seizure cipher we look at first is called a chef cipher, which is a special case of this, because we should in a tree substitution size for everything is random. Here we have a message which can be curved. Department computer science. And the entire concept of it is very easy to understand. All right, so it's almost like if we are typing on the keyboard, we know what all the letters is, but somebody comes and changes the letters on the keyboard are. So we basically have this word. It will back exactly one other word. And hopefully that was obvious fate of hybrid message enough get it right. And overall, this ends up with why did you cipher right on the basic depth. So if somebody would just present you with a lot of text, you can obviously see if you find it really just equipped it scale.

Once again, like a little example. It's fine. It actually looks quite random. Right? So the question we need to ask ourselves, how secure is this? Right? And if you think about that, we have to think about what are the different ways people can impact it? How secure would it be against different kinds of attacks? If we think back to what we say, it's a matrix encryption for us.

All right. We said that Alice involved each had a secret. If this secret is basically what makes the cipher work. When we have a shift cipher, the genius in decipher the shift cipher, what was that key? What was the thing that Alice involved needed to know the error is safe and receive the message? Any idea? The value of the shift? Alice must know she's shifting her alphabet by three. Involvement knows it should be the alphabet by three or four or five or six, or whatever that you where we have a true substitution suffer. Why is the key? We're not shutting down a bit. What is the key when we have substitutions offer for real? Any guess? Seven. Sorry. Sentence would be. So sentence, good one. So that is an example that example we chose about how we made the the Alpha date with the sentence. That means Alice and Bobo boss know the same.

If we use some other method, or if we consider the others as well, like these various methods at the end of the day, in a true substitution. So I heard the key is this alphabet. Right? So however, Alice and Bob creates it. Alice must have this alphabet, and Bob must have to set alphabet. Otherwise, they're not gonna be able to see each other Information for an attacker, for the attacker to win and decrypt Information, the attacker must be able to guess this alphabet. This method is extremely simple. We look at the concern that maybe we can write programs in case of a bit. You can just drive route for search algorithm. Right? I will sit here with that be actually, the total number of permutations we can have for this alphabet is 26 factorial, basically, 26 × 25 × 24 × 33 × 22, all the way up to 1. That's actually a massive number. It's equivalent to an 88 bit number, very large number.

If I was to write a program that's gonna good for search for the right alphabet permutation, if I had 1 million desktop PC each one can do 3 billion, such as a second, my search engine will take more than 4,000.

Now, we see that against this specific attack, with force, this very simple software is actually not that bad. In fact, even today, if the attacker could only use brute force attack, this offer would still be pretty good, in fact, better than days in terms of resistance equals attack, which is something we used up until 15 years ago, right? Some people so used. The question comes, is there anything better than we can do to crack the Cyprus? Obviously, we don't use substitution software anymore. Yet, for certain attacks is very good. What happened to substitution, cipher that made it easy to break? What is the problem with it? So on that night, before we can take a break, statement is three. So you can spend your break thinking about the price. And then when you come back after the break, and i'll talk about what we want, the substitution. Right? It's 10 to 3. You can have infinite break, and then i'll continue to make sure we attend.