Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 07
Lecture: 19

The topic that I was given is about Cybersecurity Threats, Solutions and Challenges. There is a structure to the presentation that I have prepared, but I do not mind varying away from the structure, so that we can have a lively interaction. After all, this is supposed to be an industry exposure to you, ok. We look at realistic problems, realistic problems with realistic solutions. So, and I also gathered that not all of you have technical background. So, I try to cover some of things without much technical things.

So, I added some concepts and other things which you would require to know. Now, let us start with cybersecurity. Why do everybody think cybersecurity is important? Why do not you just read this quote? The only system which is truly secure is the one which is switched off and unplugged, locked in a titanium safe, buried in a concrete bunker and is surrounded by nerve gas and very highly paid armed guards. Even then I would not stake my life on it.

Think about this. So, why would a person who has spent a lot of time studying cyberspace make a statement like this? There are certain fundamental issues about cyberspace. The first fundamental issue is, what we call as cyberspace means anything that is connected and can interact with each other, over the airwaves or the other type of waves, is fundamentally designed to be cooperative in nature. So, cyberspace is built on cooperation, coordination, trust. So, if you say I am sending you a packet, you are most welcome to receive it.

Look at any of the protocols that you have studied TCP, IP anything. There is nothing in the protocol which says, no I want to first talk to my computer, my OS, I want to receive it or not. It was not designed like that. It was designed to be a very friendly space where everybody can interact with everybody. Even now most of the protocols do not validate.

Some of you must know about the BGP routes. The biggest cyber attacks happen by BGP routes. BGP servers are the big servers in internet which decide how the internet packets move between big networks. Like I am sending a packet from India to let us say, another company in America, we cross multiple BGP routes. So, the route says I know how to go to America, everybody believes, yeah he knows.

Nobody is going to question, how do you know ? So, this is the type of trust that is embedded in cyberspace. Now when you have built a space which is, where trust is at the heart of it, how do you implement security? This is the route of all the challenges in cyberspace. So, you have created a space where trust is at the root of everything, Everybody is nice, everybody is good, how do you catch rogues in that space? Ok. With this thought let us go through briefly. So, before we start the standard part, let us go through the definition of cyber security.

It is nothing but a body of technologies, processes and practices involved in protecting individuals, organizations from cyber crime originally, now cyber warfare. So far so good. And so now you when you say, it is designed to protect, what is it designed to protect? We have to be more specific than being, you know. So, a definition does not illuminate unless until it is specific. So, usually they talk about 5 principles out of which 3 are considered as generally a triad.

So, the first one is confidentiality, integrity, availability and then there is also accountability and auditability, correct. These are the 5 principles that we are supposed to maintain. When you say I have a cyber security system in place, you are able to say that my data is secure, it is given access to people who have rightful access to it, my data cannot be tampered with, which is integrity component. So, if you tamper with it, I will know and when I want to access my data, I will always have access to it, which is availability. Accountability means I can always identify who has made changes to my data, correct.

Auditability means it cannot be tampered, whatever changes you make. I should be in a position to say, " No, you did it at that time and you cannot deny it, no repudiation and a more academic jargon, fair enough. Now, let us look at the scope of cyber security. This is a projection roughly in 2021, I am sure all of you must have gone through statistics like this. And I will tell you from my experience in industry, probably these statistics are based on 20 to 30 percent of the crimes which are actually reported.

A large number of crimes or attacks are not reported for obvious reasons, correct. So, the statistics that are built based on 20 to 30 percent itself is so staggering, Shocking isn't it, why is this happening? Because almost all the businesses are moving digital and not many businesses have thought about security in digital. Like I told you when you build a house, you first build a compound wall right, you do not build house and then think of a compound wall. In digital space is exact opposite, you first build a house and then you think of a compound wall. See, these are the challenges that we have, which is why cyber security continues to be a big issue and will continue to be a big issue.

So I do not want to go over these statistics here, I am sure you guys can read it. Now let me ask you, when do you think the first cyber attack would have happened? Let us put a date to it, a year, make a guess. Come on 10 seconds, 20 seconds. 70s, 80s okay, good answer. Just spend a moment looking at it, can you guys read it? It is too small.

Let me see if I can zoom it little bit. Can you guys read it now? There was an attack on a Soviet era pipeline. The story on how it was done, is what we can now call as a logic bomb. The Soviet could manage to build pipelines but they could not manage to build software to control the pipelines. The software they had to source from a Canadian company.

This is the peak of cold war. So the Americans have reached out to the Canadian company, planted their own programmer and inserted a logic bomb, which triggered and destroyed the pipeline which was built at a huge cost and had a very, very significant economic impact on the Russia or that time, Soviet Russia. Yeah, it is now, it is now accepted by the Americans too. So this is the time it started. So what I, what I am trying to highlight here is cyberspace, right from the beginning was never a space of peace.

So today we have a concept in warfare largely called as, no conflict no peace stage. So you have peace, you have conflict, right. Now there is something between both of them. It is called no war, no peace. So you are not really at war but you are not at peace either.

There is constant conflict going on. So this is what accurately describes the cyberspace today and cyberspace has always been like that. So that is what I am asking you to start thinking as, correct. So before we go further into a technical concepts, I thought you should have some clarity about the key concepts because without which your understanding of the whole class will be significantly impeded. So let us look at couple of concepts.

So I will try to cover broadly two important things about you know, general concept of cryptography, operating systems and networking concepts, security concepts like triad and we will also look at couple of other things. What is an operating system? If all of you know, please say that Sir we know it, I will move on to the next slide. What is an operating system? What does it do? In simple terms, it provides an interface between the human element that is sitting there and the hardware that we need to operate on. So it can be anything, it could be starting from a small raspberry pi to your own laptop so.

Correct. So it is an interface between the human and the input output and compute - three things. Correct. There is a compute infrastructure, there are input devices, there are output devices. The human interacts with the input devices, the compute connects to other devices, performs the work and displays from the output devices. This task is made super easy by operating system, which means when you say I have switched on my machine, so you interact with the operating system.

Operating system tells you," Okay my Boss, all the devices are ready to listen to your commands. Please tell me what I should do next." Play the song. Okay boss I will play.

Fetch the file. Application " Okay, here is the file." Application says, can you process this, processed. Can you send this to the speakers? Send. You see operating system is the one which runs behind. It is everywhere but yet not felt.

You think it is intuitive, just double click. Correct. So this is the heart of the cyberspace. All battles are fought in the applications and the operating system space.

Nowhere else. Correct. Now we look at another thing called as rings. This is extremely important concept. It is a hardware concept. Now when you are trying to fight for control over the devices, like for example, I want to find out what your location is. I want to be able to destroy your hard drive data.

I want to be able to steal your personal information which means, I have to have full control over your system. How do I do that? So there are two, three approaches. One approach is at the operating system level. So multiple layers of defense. Operating system creates this is kernel which means the secret room, nobody should enter.

There is user space. You are free to play inside this. You try to cross this and get to kernel space. No, I won't let you do that. But all hackers want to do that.

Correct. Because if you become the watchman, can anyone notice you as a thief? So every thief wants to immediately down the police cap and say I am a watchman now, I am watching over everything. Correct. So all thieves, which means all the hackers when they enter the computer system, they always want to abuse the operating system powers and hide in the plain sight pretending to be part of the operating system. So there are inherent defenses built in the operating system and there are also inherent defenses built even in the hardware level. But not all operating systems use them effectively.

Even now, the latest version of Windows does not use most of the hardware protections. It is important to know that this space is not attended to, even today. So when you say, you are operating at ring 0, the hardware fully listens to you. The processor fully executes all the commands you send. Ring 1, ring 2, ring 3 are restricted levels where you have limited access, limited access.

So the kernel or the operating system largely operates in ring 1 or ring 0. These are the hardware level. Clear? Now I will also touch about couple of concepts on cryptography. How many of you know what is cryptography? Cryptography is like the basic term if you understand like encrypting the message so that someone from the middle does not understand it and the targeted audience reads it, using the key or whatever.

Brilliant. So cryptography means ensuring the CIA of the message that you are sending me. It reaches me very safely, confidentiality is maintained, integrity is maintained and it is available to me. Correct? Now how do we achieve this? There are multiple ways. How do we do it in home? You and your sister will keep fighting, pretending to be fighting, shared passwords. But the challenge is let us say, we both are separated by a common distance.

How do we share the password? If you figure out a way to share the password, we can use the same platform to send the message to, right. So how do you operate when you both are separated? There is not so reliable environment between you both. Let us say, I am talking to you, we both want to exchange a message. There are so many other ears listening, how can I whisper to you, without crossing them? Maybe they may not be paying attention but can I take a risk? I will not.

So I will consider this space as compromised. I cannot. So this is why the shared symmetric encryption algorithms won't work. Now second problem, this is called symmetric encryption. Basically we both use the same key. Now another challenge is let us say, we kept on exchanging messages.

Obviously you also know the messages now will look gibberish. Let us say you are copying all the messages sitting in the middle. Today you do not know, you do not know him and you do not know me. Later one day you know. You caught hold of me, slapped me thrice, took my password.

You will be able to decrypt all the messages. Correct? Complete compromise. Another risk in this. So these are the challenges that people experienced during World War I and World War II and with the proliferation of communication technology like radio waves. Radio waves are open for all.

So this challenge became extremely critical. I am sure all of you must have known about Enigma, cracking. This is exactly what it was. And I am sure you guys understand Enigma is a single reason why the allies have won the war.

It made a huge difference. Don't forget that. And they kept it a very good secret. That is also equally responsible. Correct? Now to overcome this challenge, people came up with a very interesting algorithms. Algorithms like for example, public private key encryption.

Now imagine it like this. You have a door. In the first example we both shared the same key. Correct? I lock, you unlock. Same key. What if I have two keys, one key to lock, one key to unlock? Same way you have. So I take a simple trunk, put my message in it, lock it with your key, send it to you.

You only have the secret key to unlock it. Now your key is known to everyone, public to lock. Let us say, I am trying to send a message to you. I know with what key I should encrypt it for you. I have no idea, how you are going to decrypt it. Everybody clear on this? So everyone let us say, we all are sending our keys.

Everyone will announce their public key. This is my public key. You want to send me a message, please encrypt it with this. If you encrypt it with this, I can guarantee you that no one else would read it, except me. Same way you want to send a message back to me, here is my public key, please encrypt that message with this and send back to me. Clear? When I receive your message, I use my private key to decrypt it and my private key is safe and secret with me. Clear? Now how do we generate these private keys? We use something called as hash functions.

What does hash functions do? Hash functions take any random block of information and convert it to a sequence of random alphanumerics. Those functions are mathematically verified, to be one way. Like, I give you a big block of data, it generates one unique number. You modify one small bit, one bit in this data, the whole number changes, Point number 1. Point number 2, If you just know this number, you can never reconstruct this data back.

Clear? So today what we have is MD5 or other type of hash functions. You pass 700 MB file, it still generates 128 characters or 5 MB file, still 128 characters. Clear? Now in this example you see the cat, the image of the cat, in the image below, one whisker is missing. You could barely notice it, but look at the hash function output. So even if one bit changes, everything is changed, which is why hash functions have a great value in forensics too.

I have got a data from, I have got a file from you. Did anyone tamper it in the way? I compute hash value to check. Matching? Okay, Nobody tampered this. Which is when you try to download anything on the internet, below the download link there is always MD5 hash value. After you download, check it. Is it matching or not? If it is not matching, while you are downloading, somebody tampered it.

Clear? So it is a one-sided computation, highly efficient, quickly you can do. So this has like multiple applications. Clear? Yeah. So it looks so simple, now you can see how it actually looks. It is a pretty pretty complicated stuff and requires lot of compute and lot of effort.

Nowadays, we have hardware also for it. Yeah. Now let us look at networking concepts. When we are communicating on the network, how many of you realize how many different different types of work happen? Let us say we are talking on WhatsApp. I made a call, let us say, if not I sent you a message you on WhatsApp. Just understand how many layers of packaging happens in the data.

Just imagine let us say, we are two computers. I have sent a packet to you. Now when I say computer, who is receiving the packets? The operating system is receiving. Operating system says ok, network device give me this packet. Now operating system first question will be yeah, am I supposed to receive it or is it for someone else? Because there are so many machines on the network, you know. How do we know? So it first says ok, my MAC ID is matching with this MAC ID.

So probably my packet. How many applications are running on my platform? I may have 2, 3 LAN cards. Which LAN card should go to? Which network should it get to? I open up further and see IP. Ok, IP is matching with this. So probably this part of my network.

Then opens up one more packet and says ok, now I got this. Whom should I give it to? So it looks at port now. Port is nothing but a unique identifier for a process which is having network connection. Is it browser? Windows update? It can be 1000 other things. Just ok, this looks like a Windows update packet.

So I will give this packet to Windows update. Now Windows update is also wondering ok, is this for which user? About which file? How would I know? The further layering, presentation, application. You see each layer helps you further resolve, resolve, resolve. So that the packet that is received or sent, accurately reaches its destination. We do not understand all of this, it looks so magical but a lot of packaging happens. So the message that you send is this small, it gets wrapped, wrapped, wrapped, wrapped, wrapped, wrapped multiple times and then gets sent on the network.

So this is a mature model which came out of years of experience. We call it OSI model.

Clear? It has 7 layers, you all can see it. Usually when we call IP, TCP IP right. So here the IP is, layer is called the network layer.

MAC IDs, you know MAC IDs which are unique to a LAN card, they are the data link. And the ports and other thing come under the transport layer, TCP. TCP is control protocol basically, yeah. Clear? Just look at how the packets look wrapped up.

Now you can clearly see, the data is only here. This is the only data. Now see how much about, how much amount of Jing bang happens. So that you actually get the packet. Same with TCP, data is here. In TCP and UDP, there is a difference.

Now I am sending you a movie, I just want to say hello. Are they same? They are not same because movies are such a big file, I can't send you in one go. I have to send you in a sequence of packets. What if you miss one packet? Everything is gone, it is useless. So I pay extra attention to ensure that you receive the packets in the same sequence I sent you.

So I wait for you. Correct? Let me give an example. I have sent a packet to let us say Vinod. I have sent, I am waiting Vinod, acknowledge please. It may happen that Vinod has acknowledged, but that packet is lost.

So I don't know. What should I do? I send the same packet, but he doesn't know. So he will have the same packet two times. Will the file open? It won't. So there is a lot of coordination that is inbuilt into the protocol. In that situation, he will not accept my packet also, he will wait.

Let us say, he sent a response. Now he doesn't know whether I got it or not. What if I have not got it? Now I also have to say again, yes you sent me the acknowledgement, I got the acknowledgement. Then the loop is complete. I send okay, I have sent you packet one.

He says, I received packet one. Then I say okay, I understand that you received packet one. You say it's a three way thing. Only then we move to the second packet. So by design it is slow, but it is very reliable. Which is why, it is not used for video conferencing, audio conferencing, streaming movies.

Because the streaming movies if you lose one packet, there will be one blurred pixel. How does it matter? You can still see. If you are looking at audio packet, there will be one small 'keee' sound.

Doesn't matter. So there we use UDP packet. I keep sending 1, 2, 3, 4, 5. You will receive 1, 5, 7, 8, 9. Still fine. You can still hear, okay. So that's the difference between UDP and TCP and the regular TCP packets.

Another concept that you need to know is access controls. These also can be implemented at the network layer, also can be implemented in the hardware layer. Okay. There are multiple protocols. What is access control? You are on my network.

Who are you? How do I know? Do you have access to my network resources or not? I have a printer. I am sure even in IIT, you guys have printers. Can you randomly connect your laptop to the cable and then print? You have to authenticate yourself. So that process is done with this. LDAP, Kerberos, Radius, these are the ways to identify every person on the network uniquely.

Because if I don't identify you uniquely, I don't know who you are. Correct? Now the next problem that you all have to learn is firewalls. What's a firewall? It is a security guard waiting at the network entry and network exit.

His rule is very simple. Saab ne bola hai, ID card nahi hai tho bahar jao. Andar nahi aane dunga. Correct? ID card hai but aap M.Tech class mein ja rahe ho, aap B.Tech ho toh nahi jane dunga.

Correct? Class nau baje shuru hogi,aap aath baje aaye ho,bahar jao,nahi aane dunga. So we frame rules. Those rules are implemented very strictly. Ab dekhiye,same securitywala kaam army wala bhi karte hai, securityguard bhi karta hai, class ke bahar wala bhi karta hai,correct. Kaam me difference hai, koi jyaada dimaag lagayaga, koi kam dimaag lagayega, koi bahut carefully dekhega,koi bahut paranoid hoke dekhega, koi bahut cheezem sambhalega aapse se like, bahut cheez batao, id card dikhao, yeh dikhao, correct, so the layer of data that you consume to verify is different at every level. So depending upon this, there are multiple layers of firewall.

If I am verifying your access at a lower level, I am a layer 2 firewall. At a higher level, which means IP level, I am a layer 3 firewall. I am even able to see, yaar aapka whatsapp toh chal nahi raha yahan pe aapka packet kaise aa gaya yahan par. Toh, I am at application layer. So at each layer, you add more, more intelligence, more, more data, which means more processing and more expensive.

Toh first level firewall, bahut basic kaam karti hai. Jo security check karte hai, woh aise aise kaam karta hai Koi kuch karta nahi hai, toh us type ke firewall hai. Uparwala ekdum serious aur, CISF jaisa, ID dikhao, photo match nahi ho raha aadhar se, jao , aane nahi dunga So that level firewalls, Clear? So these are like the different layers. So I will try to cover quickly because most of the cyber security things happen because firewalls slip up. Correct? Agar firewall sahi hoga toh koi andar aayega hi nahi,correct? So, which is why it is generally important to have a rough idea about how the firewalls work.

So it is a packet filtering firewall. Woh har packet ke upar naam dikhti hai kaun hai ye, kahan se aaya, TCP IP sessions hai kya recognised IP hai kya, IP ranges match ho raha hai kya, andar aane diya, woh split karti hai, trusted network ka packet bahar nai jana chahiye, untrusted network yahan nahi aana chahiye, toh simple again basic rules implement karti hai yeh. And this is how most of the regular corporate networks look. Ek baar dhyan se dekho usko, So, router routes packet between different networks. Kaise karte hai yahan pe? Ek demilitarised zone hai, which is safe zone , wahan pe apna asset kisset daal do, koi ko koi farak nahi padta,no monitoring nothing there, aapko jo karna hai ,karlo.

So you have controlled access from outside, unfettered access through the inside, via a simple proxy. Proxy bus itna record rakhti hai ki, kaun ho aap ,correct hai, multiple networks ko connect karne ke liye, alag se separate separate routers aati hai yeh internal hai, yeh external hai, inki configurations alag, sab alag. This is how actually a, genuinely a company looks like. ab aap socho As a hacker, if someone wants to breach, what should they breach first? And if you let us say you breach something, where will you hide first? aap kahan se aa rahe ho, yahan se aa rahe ho, ya yahan se aa rahe ho, kahan se aayenge hacker, koi shakk abhi tak, no doubt na, so everybody comfortable in hindi, Who is not? Okay, I will switch out English only. So hacker will come from this side.

Fair enough so far? Let us say he broke this, where will he go next? Hide there, wait for an opportunity, then get him. Now we understand why this is very important. So any unpatch sorry, any unpatched vulnerabilities in the routers, firewalls are the cracks in your wall. Keep hitting there, it will fall. Once you get in, comfortably stay here, nobody will notice you, then get out.

I am sure all of you must have seen that movie Dhoom. If you want to catch A, you should think like A. Correct? Please. So there is one more thing called cyber espionage. If you go back to the previous diagram, so you said okay, there is one way we can take route through the routers, the networks and everything. But in terms of cyber espionage, if you really want to get into the inner workings of how the per people dynamics are working within the organization, so that in a way, you could attack the entire system rather than taking down the information assets that is there within the organization. Now you monitor the activities, how things are going on and then you do things.

So that is a different route from the other side, attacking people from the personal level, then going through the entire. Correct. See, so in that case what you have effectively done is you have directly reached here without going through the struggle because you fooled an individual employee. So through social engineering or whatever you call it, okay then you can reach directly.

So it is an easy way out but it can also be easily caught. What if you pick the wrong guy? The whole operation is gone. Correct? Cyber espionage is finished. You are totally exposed now. So there are risks and advantages. So but what we are looking at is the traditional way of looking at cyber espionage.

Now espionage or cyber warfare is just a difference of motive. You are a thief. You can also do murder, right. So you have sneaked in, got inside, you can do whatever you like. So it is just a difference of motivation but here we are looking at skill. The skill is same or is it not same.

We look at that too in the next slides, okay. Now you see how usually people connect from outside. LDAP or Kerberos, any one authentication server directly identify yourself, then you are connected to the network. So these are the gateways to enter the networks and I am telling you honestly not many people understand how they function. This explains why, despite the billions and billions of budgets that are spent, people screw up on basic things. Clear?