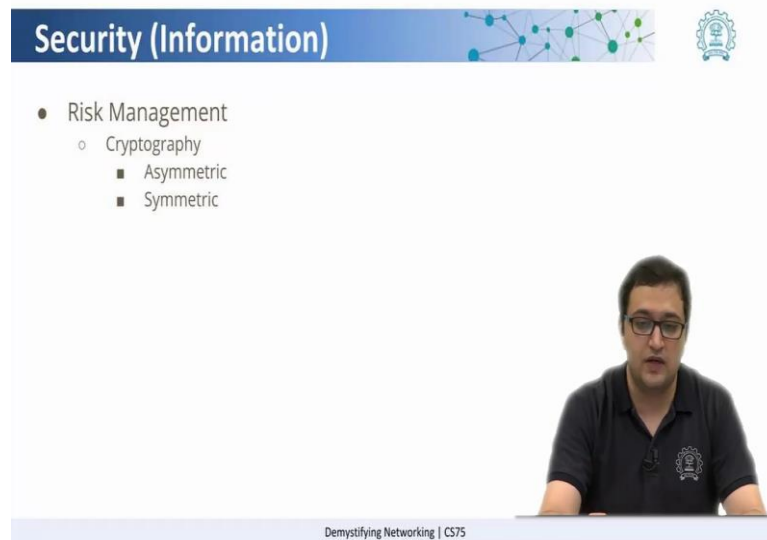


Demystifying networking
Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 77
Process Management

So, now let us come to the next point which is Cryptography.

(Refer Slide Time: 00:03)



The slide features a blue header with the text "Security (Information)" and a network diagram. Below the header, a bulleted list is shown: "Risk Management", "Cryptography", "Asymmetric", and "Symmetric". A presenter is visible in the bottom right corner of the slide. The footer of the slide reads "Demystifying Networking | CS75".

Now, cryptography as we saw in the earlier example is about changing the human readable form of the information and this is done via some complex mathematical algorithms. Now there are two types of ways that we can encrypt data, we saw symmetric and asymmetric. Now in symmetric we have one standard key which is used to encrypt and decrypt the data. In asymmetric, we use a set of keys where one of them is used to encrypt the other is used to decrypt and these days cryptography is much more complicated than what we heard about like the Caesar Cipher. Now coming to process management.

(Refer Slide Time: 00:45)

The slide features a blue header with the text "Security (Information)" and a network diagram. Below the header is a bulleted list:

- Process Management
 - Governance
 - Incident
 - Change
 - Awareness
 - Social Engineering

At the bottom of the slide, there is a footer that reads "Demystifying Networking | CS75" and a small logo on the right side.

So, what is process management? We saw that we can manage risks using these measures now we also need to have a process so, that these measures can be enforced and these risks can be avoided. So, the first part of process management says governance. So, in governance what we mean is, we need to have certain rules in place or certain processes in place so, that all of the above can be done.

For example, if we look at defense in depth, we need to have a rule in place which says that you need to secure your network, the host, the application and your data. Then we have something called the incident management. In incident management what we need to do is if there is an incident say a breach or say a failure of any system, there has to be a process in which it is recorded and reported and by recording those incidents what we can do is have processes in the future, So, we can avoid those incidents from happening.

Next we look at is change management now we saw that maybe certain incidents took place and there were certain changes that have to be brought in in the policies or say in the infrastructure. So, how do you manage the change or it could just be your updating certain systems? So, now, these systems have to be updated in a certain way so, that it does not compromise the new system that comes out after updation or while making this change information is not leaked out.

So, that part is taken care by change management, but one of the major points that we have to always focus on is awareness. We have to be aware of what the policies are why

these policies are and how do they help us and until next we are not aware of it there is always a risk. For example, something very commonly used is something called social engineering.

So, what is social engineering? Social engineering is basically looking at the human side of the company or the employees of the company and trying to manipulate them by say faking as a employee of the company or by trying to get friendly with them and then trying to extract information out of it. So, until next you are aware of why certain rules are there, why certain processes are there for example, certain companies have this policy of not having pen drives allowed.

So, there have been incidents when people who wanted to get information out of a company or say access a network what they would do is, just leave certain pen drives with some malicious code in say some common place. Now what is the first reaction that you have as soon as you find a pen drive? You just take the pen drive and try to see what data is available the moment you plug in the pen drive without your realization certain code could be executed which could compromise the security of the network. So, awareness about the policies is the key in having a network secure.