

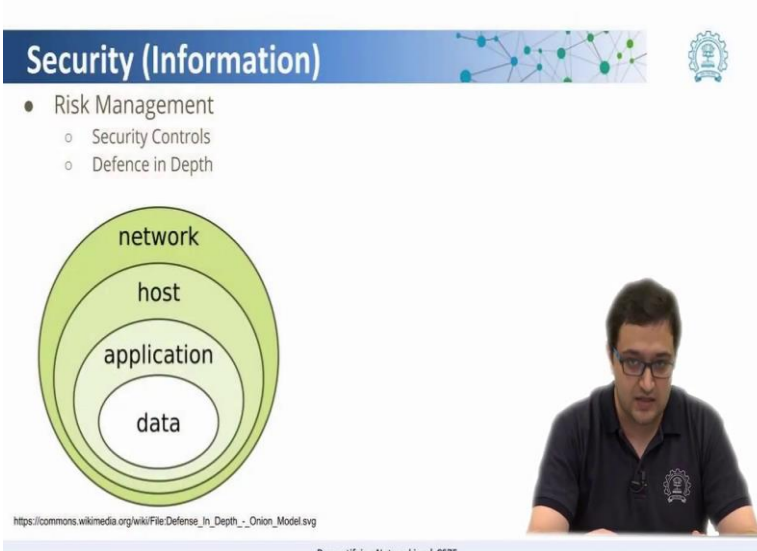
Demystifying networking
Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 75
Information Security and Defense in Depth

So, now let us look into what we call is security of information. So, what is information? Basically, when you have a lot of data, you can assimilate that data do some analysis and get some information out of it. Now, certain information are very key to certain organizations. For example, if there is a company, which has a certain set of quotes for its a new order and they have to keep it securely from its competitors so, that they will be able to win say certain projects or certain tenders. Like this example there are lot of information which are to be kept very securely. So, how can this be done?

So one of the very important thing as we talked about insecurity is, it is important to be aware of the risks. So, the first topic that we will talk about is called risk management.

(Refer Slide Time: 00:47)



The slide is titled "Security (Information)" and features a blue header bar. Below the header, there is a list of items under "Risk Management":

- Risk Management
 - Security Controls
 - Defence in Depth

To the right of the list is a network diagram with green nodes and blue lines. Below the list is a diagram of the "Defense in Depth" model, represented as four concentric circles. From the outermost to the innermost, the layers are labeled: "network", "host", "application", and "data".

At the bottom left of the slide, there is a URL: https://commons.wikimedia.org/wiki/File:Defense_in_Depth_-_Onion_Model.svg

At the bottom right of the slide, there is a small video inset showing a man with glasses and a dark shirt, likely the professor, speaking.

At the bottom center of the slide, there is a footer: "Demystifying Networking | CS75"

So, how do you do risk management? First is you need to be aware of the risks and then see what are the ways you can manage it. So, in risk management what we see is, security controls. So, what we mean by security controls is? You have certain procedures in place which help you to ensure that certain security practices are being followed. The

second thing what we look at it is defence in depth. So, in defence in depth we can look at the diagram.

So, on the diagram what we see is at the core we have the data, above the data we have the applications that are running on the data, then we have the host which is the system which is running those applications and then we have the network. So, each layer of it has to be secured. For example, the network itself has to have security like any unauthorized person should not be able to enter the network, then the host itself should be secure. Say if unauthorized person is able to physically enter the building the host itself should have security measures so that they cannot be allowed to enter the host computer.

Now, we look at the application. A malicious person is able to enter the system. So, the host's level security ensures that the physical system has been secured for only authorized access. Now when we look at application security; so, application resides on the host now if the host has been breached, so, what we can do is, have application security where only the people who are authorized to work with the application or get information and access from that application only they will be able to log into that application.

As nowadays with what we see is applications are distributed wide on the network. So, application security itself becomes pretty important at that point of time and then we have data security. So now, what we see is, most of the times applications that represent the information get the data from some say database. Now, those databases have to also be secured so that the data in the raw form can also not fall into the wrong hands. So, this is what we call defence in depth.