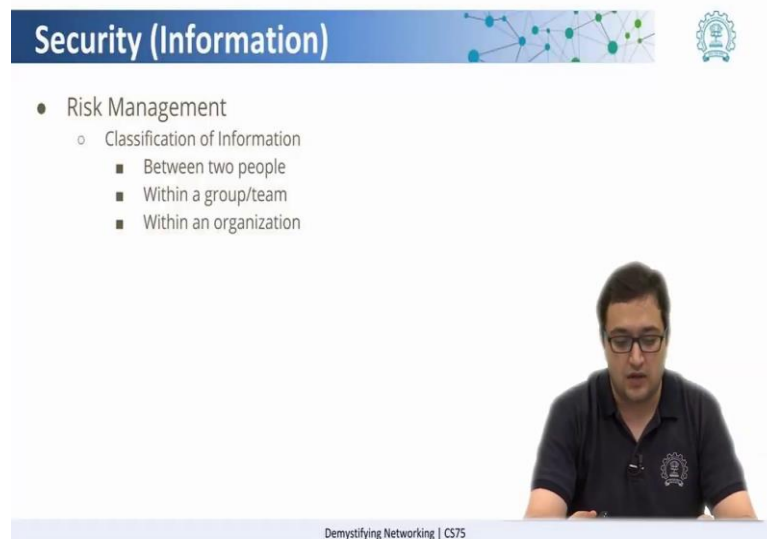


Demystifying networking
Prof. Sridhar Iyer
Department of Computer Science and Engineering
Indian Institute of Technology, Bombay

Lecture - 76
Information Classification and Access Control

Now, again when you have these information, these information have to be classified into different levels of security. So, what I mean here is we can have three levels of classification of information.

(Refer Slide Time: 00:11)



Security (Information)

- Risk Management
 - Classification of Information
 - Between two people
 - Within a group/team
 - Within an organization

Demystifying Networking | CS75

For example, we can have something which is secured between two people. So, it can be called say confidential information and some information that is secured between only a group, a group of people. So, that let's call it say a secret and there is some information which is secure only to a organization, now let us look at examples of it.

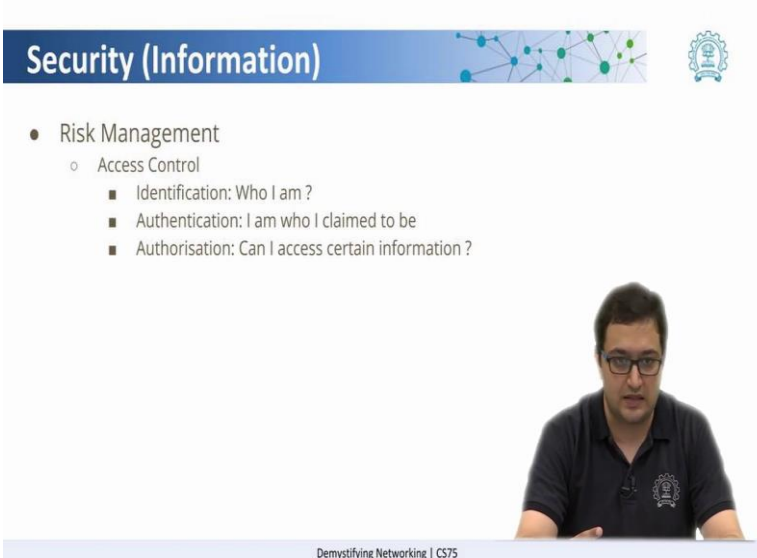
So, if there are two people who are say HR person is talking to a employee and it is something confidential about the employee, so, it is a confidential communication that is happening between the HR and the employee. So, it is only confidential between those two.

Now, the other level could be there is a particular team which is working and that team has some say user access information about the client that they serve. Now, this information has to be shared within the team, but should not leave the team.

So, you can classify this information using some keyword for the entire team, but finally, now say now we have some information which is relevant for the entire organization. So, that it is available to the entire organization. So, that can be classified at the organization level. So, here we can have keywords for each of the type of classification of the information. And why communicating? We can use these keywords to ensure that this communication belongs to a certain level of classification.

So now, we look at what we mean by access control. So, we saw that in classification information and in defence in depth, certain information which is only supposed to be available to certain set of people and how do we determine that these are the set of people or are they allowed to look at this information. So, here is where access control comes in.

(Refer Slide Time: 02:03)



The slide is titled "Security (Information)" and features a blue header bar. Below the header, there is a network diagram and a logo. The main content is a bulleted list:

- Risk Management
 - Access Control
 - Identification: Who I am ?
 - Authentication: I am who I claimed to be
 - Authorisation: Can I access certain information ?

A presenter is visible in the bottom right corner of the slide. The footer of the slide reads "Demystifying Networking | CS75".

So, access control has three things in it. It is called identification, authentication and authorization. So, what identification means, I am trying to tell who I am. So, say I am a employee of the company. So, how do I identify myself? By showing my I card or I have certain credentials or say certain employee ID that I have. So, I can be identified with that as I am a employee of this company, the second part is authentication.

So, by authentication we mean is, I am who I claim to be; that means, that if I am an employee of this company and I am the holder of this I card maybe there is a pin with the I card or if you have a username from the companies or the employee ID from the company you have a password. And, since you know the password you can claim that you are the person and in these days we have a lot of different methods of authentication. We have biometric authentication, where you can use fingerprints, you can use iris scanners and a lot of that and the third part is authorization.

So, now I have proven that I am a employee of the company and I am the person who I am who I claim to be, but am I authorized to look at this information? So, authorization actually determines the kind of access levels that you have. For example, now if I am employee of the company who works in a certain team which provides information about the human resource. So, the human resource employee is authorized to look at human resource data of a company, whereas, if I am an employee who works say at a different department say the networking department. Now, I am authorized to look at what are the kinds of information that are going around in the network say for security reason, but I am not authorized to look at the personal data which the HR person is authorized to. So, like this we can have different authorizations for different set of information. So, by access control we mean, we have to identify that the person belongs to that particular organization we have to authenticate, we have to ensure that he claimed who he or she is and finally, in authorization they have the authority to look at that particular into information.