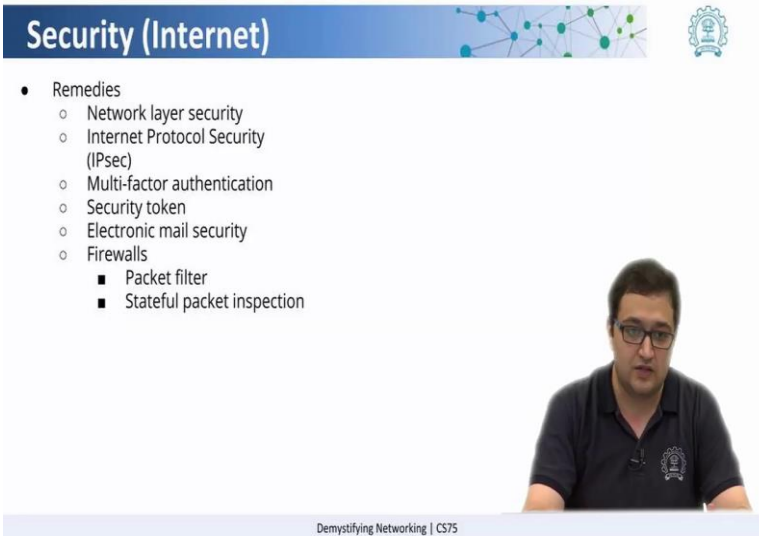


**Demystifying networking**  
**Prof. Sridhar Iyer**  
**Department of Computer Science and Engineering**  
**Indian Institute of Technology, Bombay**

**Lecture - 81**  
**Securing the Internet Usage**

Now, what are the remedies that we can have to protect ourselves?

(Refer Slide Time: 00:07)



The slide is titled "Security (Internet)" and features a blue header with a network diagram and the IIT Bombay logo. The main content is a bulleted list of remedies. A video inset shows Prof. Sridhar Iyer speaking. The footer reads "Demystifying Networking | CS75".

- Remedies
  - Network layer security
  - Internet Protocol Security (IPsec)
  - Multi-factor authentication
  - Security token
  - Electronic mail security
  - Firewalls
    - Packet filter
    - Stateful packet inspection

So, now remedies can happen at different levels. So, let us talk about say network layer security. So, on the network you can have the securities by access securing your Wi-Fi access points, then securing your management managing devices, like you can secure your routers which is or you can use a centralized system to manage the security of the entire network and then the other things are all the communication that happens on the network has been secured. By that we mean we communicate over privately, we used things like internet protocol security suit which is IPsec these days, by encrypting the information we will be able to ensure that it does not it is not readable in the human form by someone who is not authorized to read it. Then we have something called the multi factor authentication.

So, we talked about multi-factor authentication. Now if the data or the particular area that you are looking at is highly confidential or secure, you could use a multi-factor for example, you could have a pin and also the biometric data both of them to authenticate

the person. So, after multi factor authentication we also have something called security tokens, which can be used to securely access certain applications and even physical spaces and we also talk about electronic mail security.

Now most of the communication that we do happens over email. So, there are ways that you can encrypt your emails and there are services so, that the emails that are sent over the network are sent in a encrypted form so, that if the information is tapped at certain place because it all travels through a public network it is not in the human readable form. Then finally, then we have things like firewalls in place. Now firewalls are more of a defensive measures.

So, what firewalls can do is, they can filter packets based on certain properties. For example, a packet has a property of IP addresses of source and destination. So, if we know that this particular IP has been known to be sending malicious communication, we could block that particular IP or if there are certain ports which are not being used and could be a vulnerability to our system, we could block those.

Then we have firewalls which can do stateful packet inspection; that means, they cannot just look at the source and destination information, they can also look at the kind of data that is going in through or the kind of applications that are communicating through the data, like we saw port numbers. So, port numbers determine which applications that we are using and say for example, certain company wants to block certain social networking websites. So, it can actually inspect that communication and see if it belongs to a social networking website and block that.