Information Security: Level #4

Prof. V.K. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

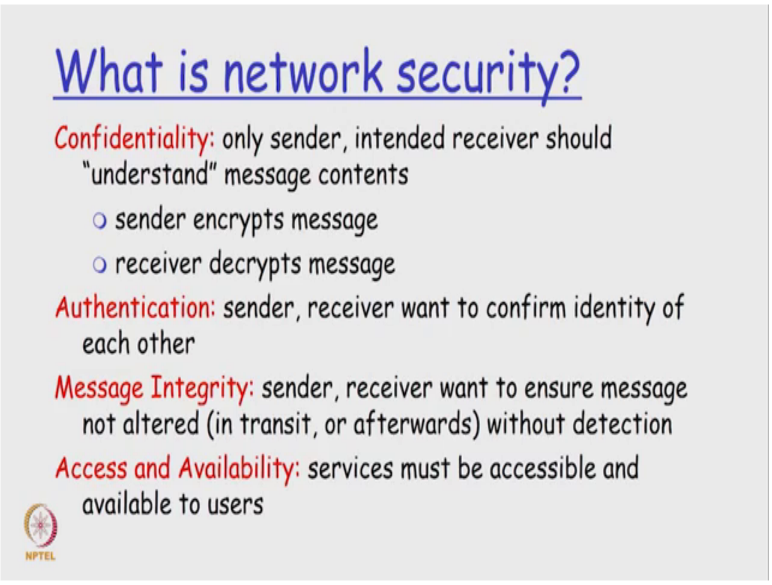
Lecture - 04
Network Security: A Re-cap

So, welcome to this session and we will be talking about network security, will do a recap of what we are done in the information security level 3 course very quickly will see. Basically, this recap will be oriented towards understanding some of the threats as we mentioned in the previous session as we saw on the previous session, many of these threats the two aspects to this one thing is that we need to protect it from not happening. And if at all it happens then you need to have a log by which you prove what is happened and you know both legally and technically what should be the remedy.

So, that should be a trace of what has happened and we need to prove that you know something wrong has happened. So, one is prevention and once and attack happens in spite of the prevention how are you going to basically address them. So, all these things these two aspects will now start looking at it from a network security perspective and also from your operating system perspective.

Now, let us look at what are all the security features that are available today that are relevant to networking. Networking essential here means that one computer gets connected to another computer.

(Refer Slide Time: 01:36)



What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and Availability: services must be accessible and available to users

The four important properties that one need to; one any. system need to satisfy when they are communicating messages with each other. One the first one is confidentiality. So, all of them in a very very broad sense in a very big viewed mail appear to look the same, but there is very very settle and very important difference between each that you are going to talk of here. The four bullet points, it is see on this slide.

First one is confidentiality: here only sender and the intender receiver should understand the message content. Please under confidentiality does not mean that I send a message nobody else would receive it. Any number of people can receive it; I do not mind many people receiving it. But, the person who can make sense out of it should be the intended receiver. Please understand that very clearly.

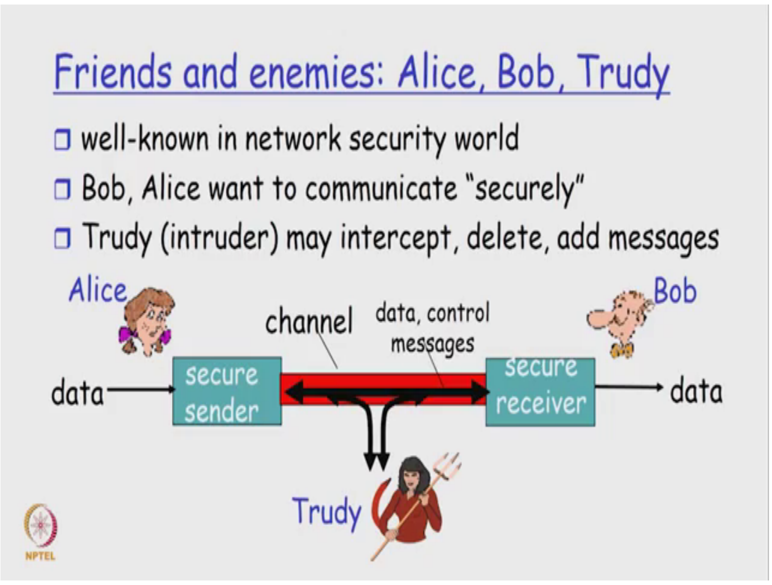
So, confidentiality essentially means it is not that I send a message nobody else should receive it, anybody can receive it, but nobody should understand except the intended receiver. And how to do we achieve this? As a sender I encrypt that message, meaning I jumble that message and the receiver de jumbled this message what you call as decrypting the message and basically take the; we the exchange the message in this fashion. The other fellows who have got this message will not know how to de jumble it or do not know how to decrypt it and so they will not understand what we both are talking. So, this is what we mean by confidentiality.

The second thing is authentication. Hear the sender and the receiver want to confirm identity of each other; you have alone sent it, it is not somebody else trying to send it to me. So, that is what is called as authentication. So, two people agreed to set, two people are exchanging communication and one fellow receives it say b receives from a right, b receives a message yes ensure that it is in these send by a and not somebody cloning or acting like a. So, that is that comes under the second point what we called as authentication.

The third point is message integrity. The sender receiver want to ensure that the message is not altered I send a message nothing should change in between the receiver should get exactly that message if he is not getting it something somebody is tampered it then you should know that somebody is tampered it. So, that is called integrity and the fourth important thing is access and availability when we make a system where we can send this messages ensuring confidentiality authentication and message integrity, but many times if this system is not be accessible or it will not be available then there is no use. So, I need to send a need to send message to b in such a way that it should be represent it anytime that is what the four point say fourth point say essentially axis and availability.

So, I should be in a position to send the message at any point of time and while sending this message I should maintain confidentiality. In the sense that when I send a message intended for be only b should be in a position to understand what I have sent and second thing is b should be in a position to also certify that I have actually send the message and nobody else on my behalf. And the third thing is the message I sent exactly as list to be without any change right and this should be possible at any point of time and this is where; these 4 points namely confidentiality authentication message integrity access and availability means.

(Refer Slide Time: 05:03)



Friends and enemies: Alice, Bob, Trudy

- ❐ well-known in network security world
- ❐ Bob, Alice want to communicate "securely"
- ❐ Trudy (intruder) may intercept, delete, add messages

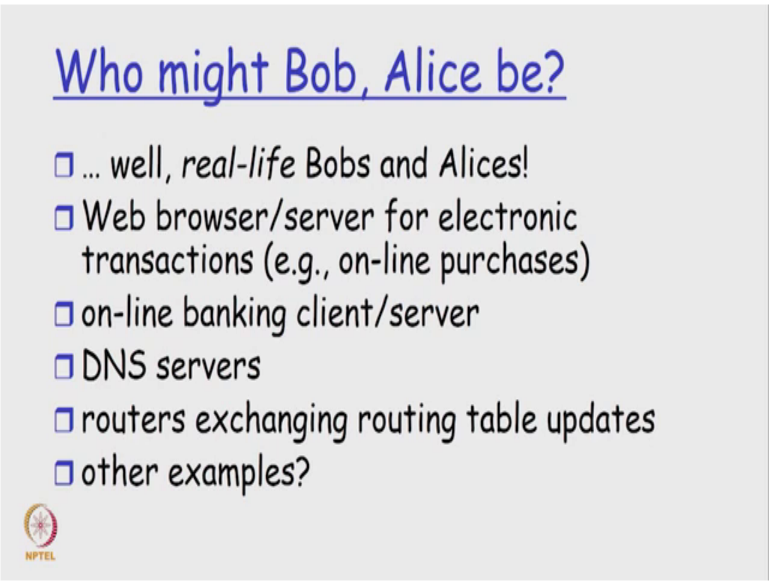
Now, in a network when two people are trying to communicate they are friends and there are people who are who want intercept and understand what they communicating and we call them enemies. So, in the literature of cryptography this Alice and Bob are always friends and there we a Trudy whose always an interceptor. So, the image that you see on the screen is as follows.

So, there is an Alice who wants to send a message to Bob, right and they send it they have a secure sender meaning they encrypted a secure receiver which decryption. So, the data is sent, but there is a Trudy who is sitting in between who just gets whatever you sent and try to interpret what has it represent. So, the Trudy is basically and interceptor trying to understand what Bob is Alice's Alice and Bob are trying to communicate with each other now Trudy is a intruder you may intercept what Trudy can do if we not just understand what the messages maybe it is not even interested in understanding that message you can just basically intercept and delete the message or you can add some new message on behalf of Alice.

So, interceptor is not one who is always interested in understanding what a is communicating with b it. So, that is one way of attacking the system, but the interceptor can be one who can basically go and just delete the message do not allow any message from Alice to go to Bob that sometimes, we call it as denial or service right or it can also say that it will add some more message and saying I am I Alice and it can send some message to cheat bob. So, this is an another way of cheat.

So, in today's network we have friends who want to communicate between each other, and their enemies who want intercept this and do not just understand what they are communicating with do many more thing like just dropping that message pulling out that message or adding new messages. So, who are this Bob and Alice are always there all human beings are there can be something else.

(Refer Slide Time: 07:11)



Who might Bob, Alice be?

- ❒ ... well, *real-life* Bobs and Alices!
- ❒ Web browser/server for electronic transactions (e.g., on-line purchases)
- ❒ on-line banking client/server
- ❒ DNS servers
- ❒ routers exchanging routing table updates
- ❒ other examples?

So, that is a very important question many times this Bob and Alice are actually systems are processes that are running in systems what is the process? Process is nothing but a program in execution have covered this and information level two course architecture right to information security a process is nothing, but a program in execution ok.

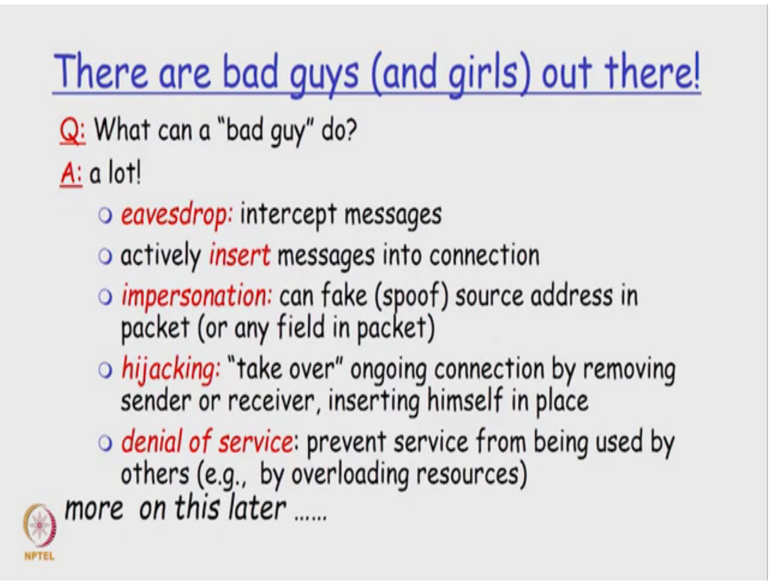
So, the process is here can be Bob and Alice right. So, a web browser or a web server for any electronic transaction or online purchase can act as a Bob and Alice. So, the so, I have a web interface I type something he is Bob and or Alice and he sending a message to other person would be a web server is capturing this message and doing certain action, right. So, a web browser and server can a good examples of Bob and Alice and both of them are basically not really human ok.

For example, if you look at online banking the client and server there again Bob and Alice we are something called DNA servers which basically resolve the name domain name server service and then here can be somebody who some other server which is requesting or some other interface network interface which is requesting for a particular name. So, both of the both the end need not be human beings similarly that can be multiple routers on the internet they may be exchanging some routing table is some routers expire; so, just deleted. So, some routing table related updates these two routers will be exchanging and that is also an example of Bob and Alice.

You can think of many examples where there are no human beings, but there are process is basically program in execution that are basically trying to communicate over a network and they want that that communication to be secured you can think of many other examples also I have given you some five examples you can think of more examples and I want an active participation in the web in the in the discussion forum on what would be possible Bob and Alice right.

So, I want the team to start discussing now we have Bob and Alice need not be really human beings they could be processes which are program in execution running on two different systems.

(Refer Slide Time: 19:44)



There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

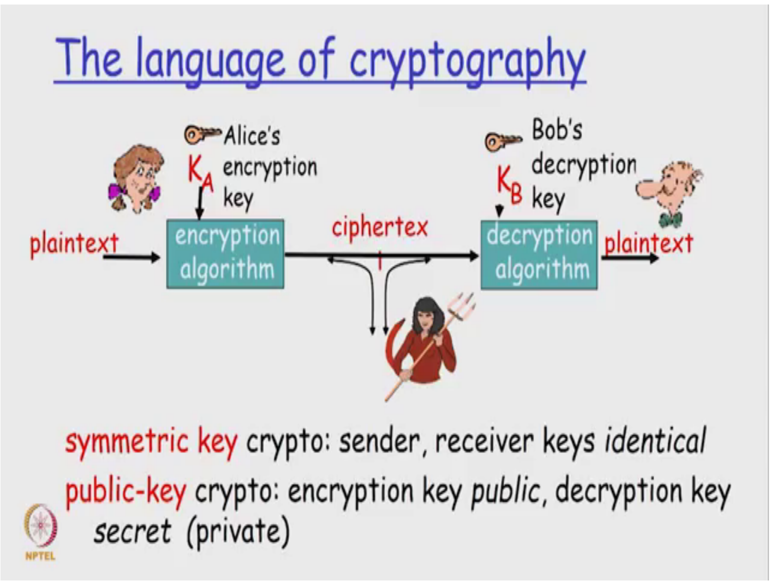
more on this later ……

Now, there are bad guys girls out there who will be intercepting this message and what can they do what do you mean by intercepting taken too many things. So, let me just give you say some five interesting things first thing is eavesdrop drop I will just intercept the message what I do with this is next, but I intercept it another thing is I can actively insert messages into the connection new messages can go there and while doing this I can also impersonate this is call spoofing or what you call fake; fake the source address in the package. So, when Alice is communicating to work the Trudy can become an Alice and send some message to Bob. Bob will think oh Alice is sending a Alice is are responding and then we can interpret the problem hijacking; hijacking is takeover ongoing connection by removing sender or receiver inserting himself in place, right.

So, Bob is trying to communicate with Alice just move Bob and put yourself and start acting as bob. So, Alice will start communicating with you as if your bob, but you are actually an intruder and the real Bob will things that oh Alice has just left the session and you will log out. So, somewhere this is called hijacking and the thing is denial of service just drop the packets. So, a Bob no packet from Bob will reach Alice and visa-versa. So, that are five interesting or important things not necessarily interesting, but really its carry things that that a bad guy I can to a Trudy can do eavesdrop insert new packet impersonate on some pa hijack somebody and do a denial of service will see many more things as we proceed in this course.

Where we talking of these things because these are very very important for us to basically understand how we can do a network forensic do not. Now how does? So, let us go back to the first issue of confidentiality how does Bob and Alice communicate with each other assuming a open network that many people can get the communication, but only the intended party can decrypt it understand what the communications is. So, this is the real problem that is the first problem that we have talked of namely confidentiality. So, there are. So, the language of cryptography used two types of ways by which an which we can handle it absolutely the only want something that is common between these two cases that when I start communicating when Bob start.

(Refer Slide Time: 12:14)



The language of cryptography

symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

Communicating; they have to encrypt it, encrypt the message using encryption algorithm for doing this and then what happens when Alice start communicating in this slide it gets encrypted when Bob received it we decrypt it. So, decryption and encryption or same for both the two types of cryptograph that we are going to introduce namely symmetric key cryptography and public key cryptography both the symmetric key and public key cryptography assumes that when bobs Bob or Alice sent a message to the other person they sent it basically using encrypting it one end and decrypting on the receiving end encrypting on the sending end and decrypting on the receiving end.

So, a plain text is given to the encryption algorithm is gets encrypted that encrypted thing is called cipher text the cipher text is not decipherable by anybody and then at the end the entire thing is decrypted and again the other party intended party gets the plain text ok. So, now, what is important for the encryption and decryption algorithm you need something called a key. So, you encrypt using a key and you decrypt using another key these two keys have to be compatible.

So, if I use the key for K A for encryption by Alice Bob will use a K B for decryption for the same message and this K A and K B must have something in common right if K A is equal to K B, then this is called symmetric key cryptography if K A is not equal to K B right, then it is called asymmetric key cryptography and one part of this asymmetric key is called public key cryptography where in the encryption key is public everybody can know the encryption key while the decryption key is secret or private in the case of symmetric key both the encryption key as you see in this slide K A and K B are both private that is what will happen in symmetric key and where K A is also equal to K B.

So, you will have only one key which Bob will know and Alice will know and they will decrypt, but on the other hand a public key cryptography is K A will be known to the entire world K B will only to Bob ok. So, this is called public key cryptography. Now we will understand the symmetric key and public key cryptography the implementation part we are not going into the algorithm algorithms. You will learn it in a crypto course, but will just go into the implementation part understand how this system works and that is what we will take forward.