Decompilers

The presence of metadata in .NET assemblies makes it feasible to decompile an assembly back to C# code.3 There

are a few decompilers available; I’ve been using DotPeek from JetBrains recently.

first of all, what are the three main goals of cryptography? Essentially, as we say it to CIA, that is – confidentiality, integrity and availability; so the goals are essentially as follows, like hiding the information from unauthorized access, that is - a person or user who is not authorized to use a particular piece of information should not be able to access the information. Integrity of data is important, that is, the information should be prevented from modification, by a person who is not authorized to do so.

We all know that we always do modification of data. For example, typically, in a bank scenario, where we try to kind of debit an account or credit an account, then we are continuously changing our balances, but imagine like, if instead of me updating my bank account, somebody else does; so that is not proper; so that is an illegal use. So, cryptography also tries to provide the integrity of the information, which is there in my bank account; so, that is what is meant by integrity.

The other important thing is availability; so, therefore, while doing all these or rather while taking measures to achieve the goals of confidentiality and integrity we should not make it so clumsy - like the network should not be nor the communication should not be so clumsy, that the information is not accessible to the authorized user.

So, by saying that it is not accessible or it is rather not available easily means that it may become very slow. For example, you are trying to access particular information and imagine that it is so slow that you cannot access it, therefore it is not usable.

So, therefore, the objective of cryptography is to provide confidentiality and integrity of data while maintaining the availability of information to an authorized user.

Now, we shall consider the typical scenario of a cryptographic network. So, therefore, there are two users, or as we say, legal users or authorized users. Consider Bob and Alice, as we have discussed in the last class, they are the two most popular characters which are used to describe a cryptographic scenario, and they send information like suppose, Dear Alice. So, there is an eves-dropper who is unauthorized to obtain the information; so the eves-dropper essentially has got an access to the communication channel. And Therefore, what is believed in this set work, or rather, in the setting is that this communication channel is not trusted; so it is an untrusted communication channel through which Bob and Alice tries to communicate a piece of information.

The goals which cryptography tries to provide are, as we have discussed, confidentiality, integrity and availability of information; that means, eve should not have an access to this information, so it should be some sort of unintelligible to the eve, and at the same time it should not be able to modify this piece of information. Like, instead of saying dear Alice, it should not be something else; so that there is a kind of misunderstanding between Bob and Alice. At the same time, Alice should be able to access this piece of information easily. So, it should not be that the network becomes slow or the packet is dropped, in order to prevent it from being accessed by eve, and in the process ending up

in Alice not being able to access the piece of information, so that should not happen; so the piece of information should also be available to Alice.

So, these are the basic three broad goals which cryptography tries to provide to users. We have to see that what are the mechanisms that cryptography or network security or the subject essentially, provides to achieve these goals?

Now, we shall little bit look more deeply into each of these topics. So, we can see for example, confidentiality; confidentiality is essentially, where the information is exchanged over untrusted network. As we have said just now, that the information is being exchanged over untrusted network and we have to provide confidentiality in such a setting. So, therefore, the information, while in exchange should remain secret

Therefore, when we are kind of exchanging a piece of information, then it should not be opened up to a person who is not supposed to use this information. At the same time, confidential is related to both the storage as well as transmission of information, which means, that it is not only like, when we are storing a piece of information, but confidentiality has to be provided in transit; that is, when the message is being passed from say, Alice or Bob or over an untrusted network, it should be confidential and it should not be opened up to person like eve, who is not authorized to use the piece of information.

(Refer Slide Time: 05:55)

So, then comes the topic of integrity, as we have discussed. We know that information is always changing. The basic objective of having information is one of the objective is like, to kind of, modify this information; so information is always transient, but the thing is, it should be made by only the authorized users.

So, imagine I do a railway booking, or for example, as I said that I have a bank account, and this information should be only changed by the people who are authorized to do so. But what we term in this literature as modification means, that change which is made by unauthorized user. So, therefore, these unauthorized users can be given various names like attackers, it could be hackers, it could be people who are kind of trying to sabotage this piece of information by modifying.

So, for example, I have a bank account and somebody else continuously extracts money out of it; so that is the piece of modification which needs to be stopped. So, therefore, we need techniques to ensure the integrity of data, that encompasses essentially two parts: the unauthorized users should be prevented from modifying this piece of information and also if somebody does any modification, the second line is, I should be at least able to detect that the modification has taken place, and try to identify who has made this modification.

So, these are kind of the two important goals which essentially needs to be satisfied by cryptography and is needed by any form of e-commerce or electronic transactions; so these are very important goals which cryptography needs to satisfy.