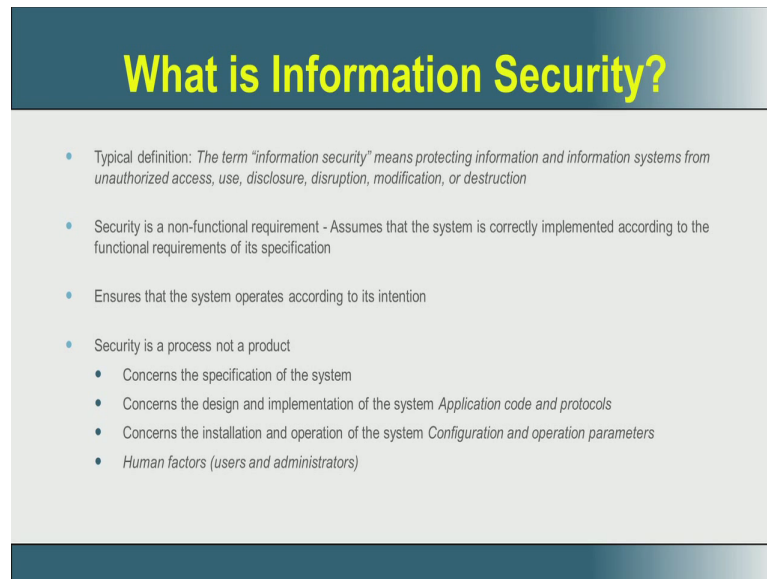


Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 03

Hi, in this session, we will be defining certain terms.

(Refer Slide Time: 00:10)



What is Information Security?

- Typical definition: *The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction*
- Security is a non-functional requirement - Assumes that the system is correctly implemented according to the functional requirements of its specification
- Ensures that the system operates according to its intention
- Security is a process not a product
 - Concerns the specification of the system
 - Concerns the design and implementation of the system *Application code and protocols*
 - Concerns the installation and operation of the system *Configuration and operation parameters*
 - *Human factors (users and administrators)*

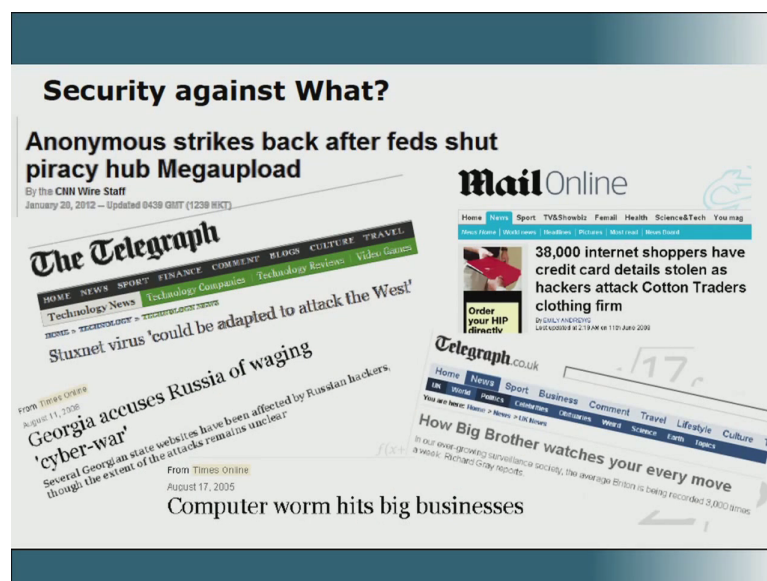
In my opinion, the entire problem of security today – why certain security needs are not complied with; why there is a lacuna in implementing certain security policies? One of the root causes of this is people don't understand the definition of different terms that are involved in information security. So, this session, we will basically concentrate on defining what we term as information security. Lot of people have attempted to define information security. The term information security actually means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. So, this is the definition that is popularly given for information security. But, let us go and understand; let us split this word security, information. First, we will go and define what is security, because security is more closure and more practical for us to understand.

First and foremost, when you look at a working of a system, there is something called a normal functioning of the system. Security is not reflected in that normal functioning of the system. In the sense that, security is not a functional requirement; security is something which monitors the function, which guides the function, so that certain

properties are not violated. So, in principle, when we try to implement security policies, one of the basic assumptions is that, the system is correctly implemented according to the functional requirements of the specification; and that, the system operates according to its intention. So, security is a completely non-functional requirement, which basically tries and monitors how certain things are happening inside the system. In some sense, we have a product say we have a core banking product, which basically takes care of your database and your access to the database; like that, the security is not a product; it is actually a process. And, security is not concerned with one aspect of the system; but, it is actually more concerned with every aspect of the system.

For example, how the system is specified; how the system is designed; how it is implemented; what are all the different application softwares that is running on; and, how these application softwares communicate with each other; what sort of protocols they use; what are the actual hardwares that were used in an implementation; what are the configurations that are set on this hardware; how do these hardware operate; what are the versions of the firmware that is installed inside the hardware, all these are concerns of security. So, we cannot pin point that, security is a specific product which does all these things; but, security is all pervasive inside the system. And interestingly, human factors also contribute lot to the security. Who are the users; who are the administrators; and, how are they aware; how do they behave from a security point of view; are they strong; are they aware of the different security policies. All of these are concerns for security.

(Refer Slide Time: 04:31)



First and foremost, let us go and understand what are we securing ourselves from. Now,

you see at least 5 case studies, 6 case studies that we have put on the slide. The first one on the top was this mega upload problem, where there were lot of free media, free movies, free software that were uploaded into one particular site. And, people downloaded it, because people like watching movies. But, what came as a quote and quote price was that, along with this software, along with this media, along with these files, came the malware and they were installed in the systems. So, this is completely anonymous; nobody actually knew, it was very indirect; and, people actually we can say they purchased at a free cost, the malware.

The second interesting thing was the Stuxnet, which was just because of improper security processes, wherein the whole software – the entire network was not exposed to the internet; but, the whole software spread due to usage of USB drives. This need not be just commercial or technical; but, this can also be political. Like for example, Georgia accuses Russia of waging cyber-war. It can also be that, it is not that it goes... And, security does not mean that, something gets corrupted; but, I also give a denial of service. For example, I want to access data; I am not allowed to access data. And, that is what was done in the computer worm, which actually hit big businesses. The other thing was that, I am not interested in corrupting data, but I am interested in what you are doing – sniffing. And, this is what you see in that article, how big brother watches your every move. Then, is of course, the confidentiality or the privacy; you have a credit card; the details inside are private; and, people are interested in stealing that private data.

So, if you look at all these 6, there are different... These are all different facets. One is I don't even make data or the service available to you. It is a question of availability. Somewhere I make the data, that is there, not integral. For example, the mega upload; I am just looking for a movie; but, what is there is movie plus some malware. And, in the case of the credit card, we have lost our confidentiality. So, the security is now against three parameters; if we can see here, it is against confidentiality of data or information; it is against integrity of the information; it is also against the availability of the information. So, what are we trying to secure ourselves from, is a very important question. Now... So, security essentially has different facets. So, we have some understanding of security in the last two slides. Now, we will go and talk about information. First and foremost, information is an asset.

(Refer Slide Time: 08:21)

Information is an Asset

- ◆ **INFORMATION ASSET” as defined in section 2(f) of the Information Technology Act 2000 -**
- ◆ **All Information resources utilized in the course of any organization’s business**
 - ◆ **includes all information, applications (Software developed or Purchased) & Technology (Hardware, System Software & Networks).”**

As per the information technology act 2000 section 2 f, this is the definition given for the information asset. An information asset is – includes all information resources utilized in the course of any organization’s business. So, the information resources include the information itself plus the applications that process this information and the technology that on which these applications run namely, the hardware. So, if you look at... There is a clear error key; there is information; there are applications specifically developed or purchased to process this information. And then, these applications software run on an existing hardware and software system; and, they are connected to through networks. So, you can see information being processed by applications software that is developed or purchased, which in turn runs on a compute system, which has a hardware and operating system; and, these compute systems are connected through networks. So, this is how from an information security point of view, we can define an information asset.

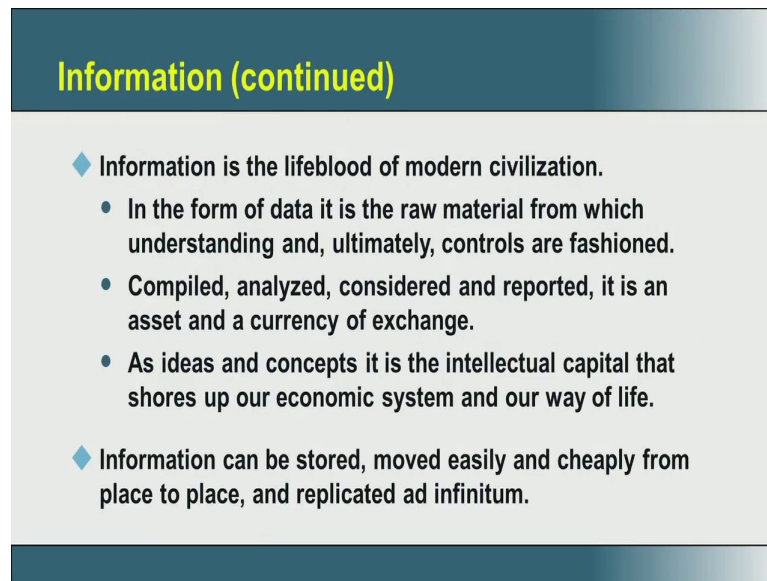
(Refer Slide Time: 09:43)

What is Information?

- It is a form of knowledge that we acquire through education, communication, practical experience, research, analysis.
- It consists of data, facts, and conclusions.
- To the engineer it is any data that can be expressed as a sequence of ones and zeros.

So, what is information? It is actually when data – raw data – when it is actually interpreted and it is used for making some business decisions, then essentially, it becomes information. So, it is actually a form of knowledge that we acquire through education, communication, practical experience, research, analysis. So, this information actually consists of data, facts that you could interpret from the data and conclusions that you could arrive at. For an engineer, it is any data that can be expressed as a binary string; but, for a business analyst, who performs some business analytics to get, make some basic decision, information is actually a form of knowledge. So, he sees information as a data on which there are facts that are interpreted; and, from those facts, we could come to some conclusions.

(Refer Slide Time: 10:52)



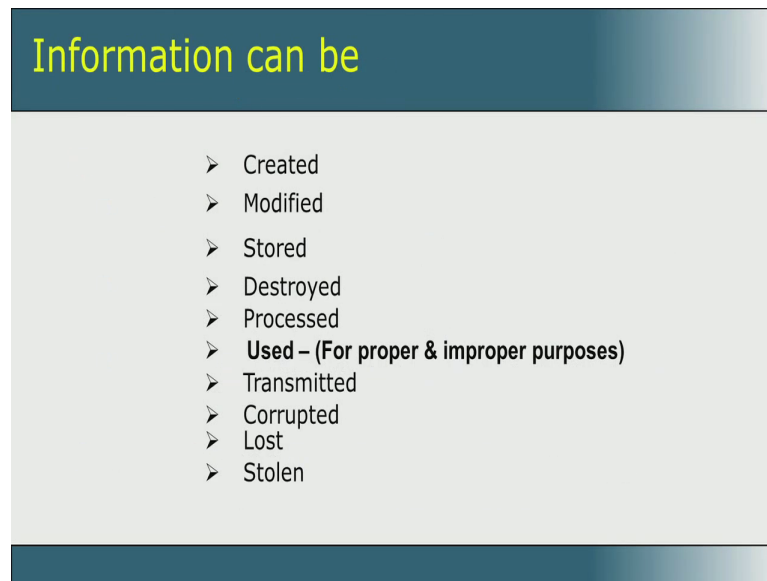
Information (continued)

- ◆ Information is the lifeblood of modern civilization.
 - In the form of data it is the raw material from which understanding and, ultimately, controls are fashioned.
 - Compiled, analyzed, considered and reported, it is an asset and a currency of exchange.
 - As ideas and concepts it is the intellectual capital that shores up our economic system and our way of life.
- ◆ Information can be stored, moved easily and cheaply from place to place, and replicated ad infinitum.

For the modern civilization, this information is the life blood. It is raw material from which understanding and, ultimately controls are fashioned. There is a huge both research and practice in the industry involved in processing information that will basically go and make an organization make business decision, make money, bring out efficiency in their process. So, data – information is something that is the lifeline for many of these organizations. Today, the word intellectual property has come up very big. So, what is intellectual property? It is again collection of information that is known to a particular organization through which it makes a business, it makes living. So, ideas like intellectual capital become very very important in this point; and, it basically dictates the economy of their country.

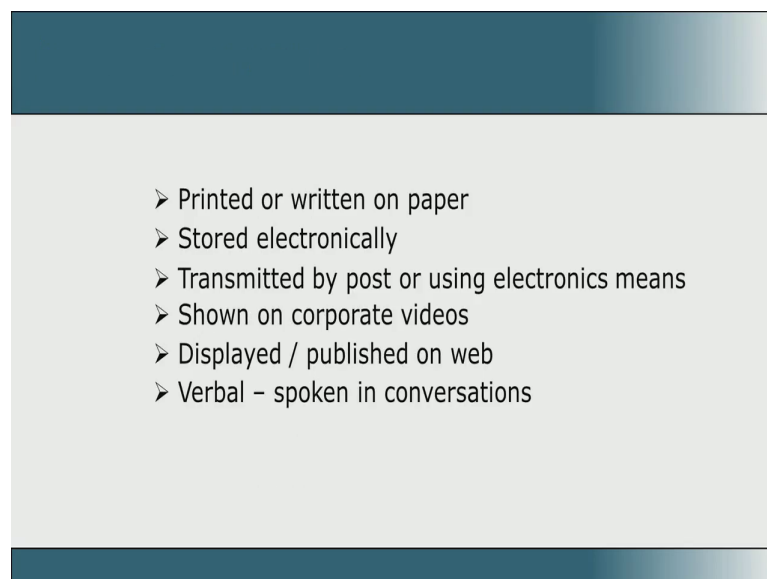
The economy of an organization, economy of several organizations put together can even make the economy of the country. So, information is the life blood of the modern civilization. Now, this information... One of the important thing that we note – why information security becomes very important is, that is, information can be stored, it can be moved easily and actually very cheaply from place to place; and, it could be replicated as many number of times I want. So, this is something very crucial about information.

(Refer Slide Time: 12:47)



So, what can you do with this information? The information can be created; it can be modified; it can be stored; it can be destroyed; it can be processed; it can be used for proper and improper purposes; it can be transmitted; it can be corrupted; it can be lost; it can be stolen and much more.

(Refer Slide Time: 13:10)



It can be printed or written on paper; it can be stored electronically; it can be transmitted by post or using electronic means; it can be shown on corporate videos; it can be displayed or published on web; it can be spoken – verbal. So, these are all the things that you can do on this information. And, suppose I want to maintain confidentiality of that information, I want to maintain some amount of integrity and I want to make the

information available; then, I have to look at all these operations and ensure that each of these operations are adhered to some rules imposed by confidentiality, integrity and availability. And, that makes the challenge for information security.

(Refer Slide Time: 14:09)

Critical Characteristics Of Information

The value of information comes from the characteristics it possesses.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

25

Now, let us look at the value of information. The value of information comes from characteristics it possesses. So, what are the characteristics or attributes of an information? Why do you see? What is the... I say it is a very valuable information. What I mean by that term? First and foremost, we should look at these seven important characteristics of information. Number one is availability. People who need this information, who are authorized to need this information, they should have access to this information whenever they want without any interference or obstruction; and, they also need it in a correct format. And, that is what we mean by availability of an information to an user. What is that... Please note that, every word that is uttered in that defining of these characteristics is very very important for you to appreciate information security.

Let us go to the next term namely, accuracy. Accuracy means free from mistake or error; and, having the value that the end user expects. So, if the information contains a value different from what the end user expects; then, it can be due to some intentional or unintentional modification of its content and it is no longer accurate. So, the user has an expectation; it can be a scientific type of expectation; I need the answer accurate to last four digits. I need an answer that is accurate as far as say last night 10 PM. So, it can be temporal, it can be in terms of the accuracy, in terms of mathematical accuracy; it can be accuracy in terms of by which time I should have taken the data, etcetera.

The next point is the authenticity. The authenticity is the quality or state of the information being genuine. Is it an original information or it is fabricated or reproduced from somewhere? How authentic is this information? What does it mean? So, what is authenticity essentially imply? It means that, is the information originally created? Where was it placed? Where was it stored? And, how was it transferred? All these things essentially imply authenticity. If I store at a very secure place; if I transfer to a secure network; then, the information is authentic. If the place where the data, the hard disk or the data center, where the data is stored is not secure as per certain norms or that transportation or the transferring of the data is not to a secure network, then the data is not authentic.

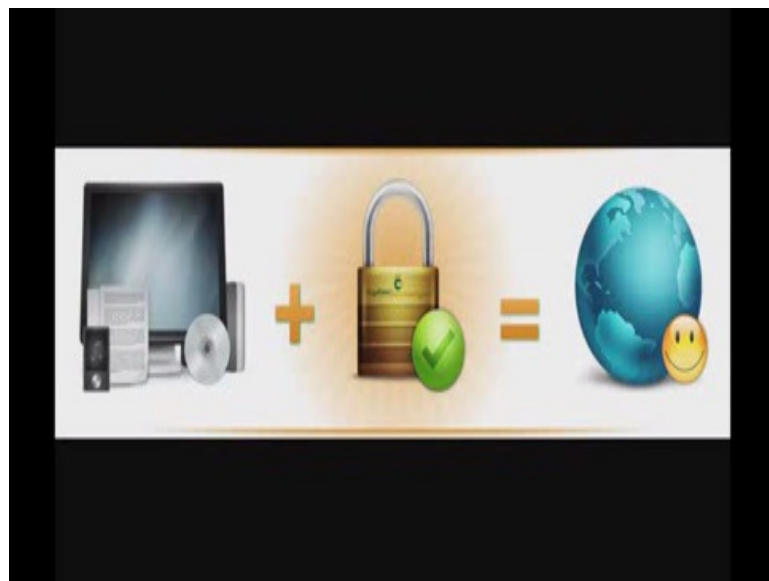
Confidentiality is defined as the quality or state of preventing disclosure or exposure to unauthorized individuals or systems. Integrity is the quality or state of being whole, complete and uncorrupted. So, what could happen to a data? It can be corrupted; that means, it can be damaged, it can be destructed, or other disruption of its authenticity. If the data loses authenticity, if the data is corrupted or it is damaged or destructed; then, it is no more having the property of integrity. Then, the utility of the data; it should be used for some purpose – some meaningful purpose to the end user. And, it should be available in a format that is meaningful to the end user. And, that is what we term utility of the data. Possession of the data; I get access to the data; I have ownership to the data; that means, I possesses data.

Please note that, if an unauthorized user possess data; that means, there is a breach of confidentiality. So, if there is a breach of confidentiality, then there is a breach of possession; that means, somebody who should not have that data has that data. On the other hand, somebody has a possession of data; it does not imply that, there is a possess... If somebody has a breach of possession, it does not mean there is a breach of confidentiality. In some sense, if somebody who should not have the data, has the data, but it is in an encrypted form; then, the end user – the user who has this data cannot do anything with this data. So, a breach of confidentiality implies a breach of possession; but, a breach of possession does not imply a breach of confidentiality. Why I made this last statement is to tell that, all these 7 are highly coupled with each other. The heightening of one can lower the other; or, the heightening of one can enhance the other. So, all these 7 characteristics are very tightly coupled. And, understanding this coupling is also very important for us to appreciate information security.

(Refer Slide Time: 20:25)



(Refer Slide Time: 20:27)



(Refer Slide Time: 20:33)



(Refer Slide Time: 20:38)



(Refer Slide Time: 20:44)



(Refer Slide Time: 20:50)



(Refer Slide Time: 20:56)



(Refer Slide Time: 21:02)

