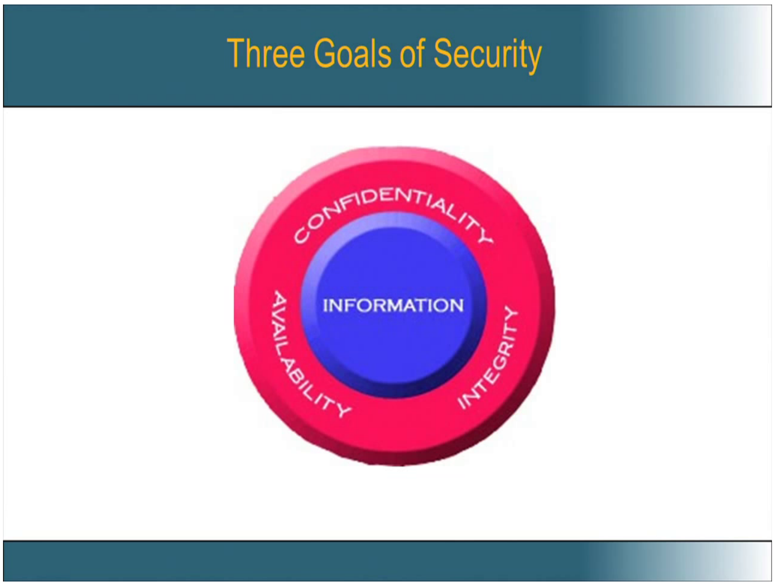
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 05
Three Goals of Security

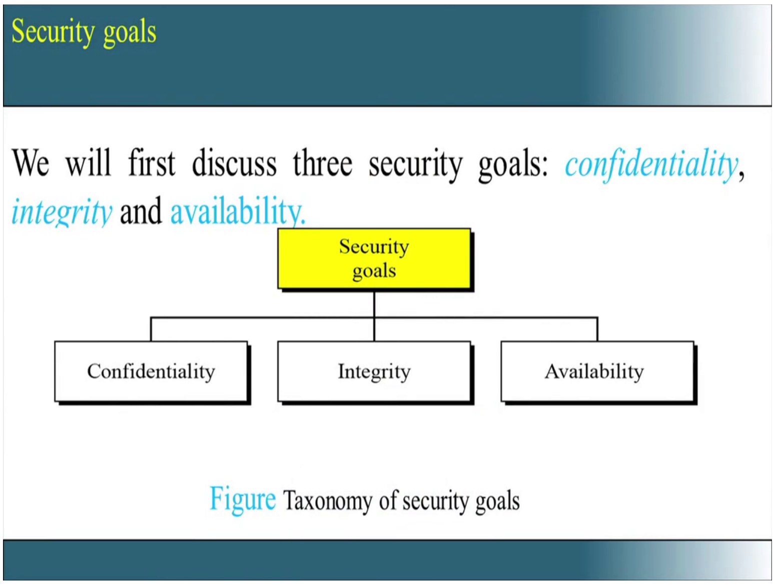
(Refer Slide Time: 00:10)



Three Goals of Security

Hi. So, in this session we will talk about the three goals of security, namely availability, confidentiality, integrity. The CIA actually forms the basis of information security. We will go now and give definitions for these three goals of security. As I told you the main problems that crop up because of security are due to people not understanding that definitions of different terms, terminology that are involved. If you have very a good understanding of the terminologies, then information security as a problem is half solved or more than half solved. So, at every stage we will spend some time to understand each of these terminologies in great detail, and we will come out with very close accurate definitions for these terminologies.

(Refer Slide Time: 01:25)



Security goals

We will first discuss three security goals: *confidentiality*, *integrity* and availability.

Security goals

Confidentiality

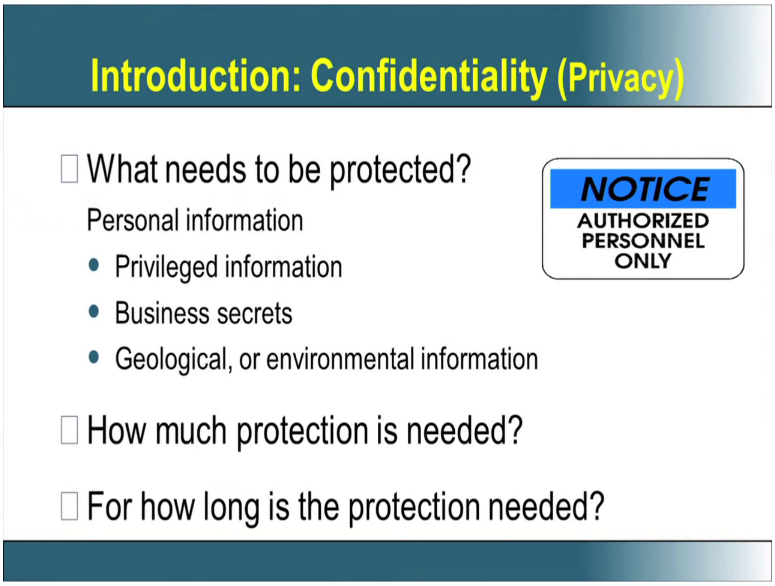
Integrity

Availability

Figure Taxonomy of security goals

So, let us start with defining confidentiality, integrity and availability. All these three formed the basis of information security and they are the information security goals, and we will now go and define this taxonomy.

(Refer Slide Time: 01:44)



Introduction: Confidentiality (Privacy)

□ What needs to be protected?

Personal information

- Privileged information
- Business secrets
- Geological, or environmental information

NOTICE
AUTHORIZED
PERSONNEL
ONLY

□ How much protection is needed?

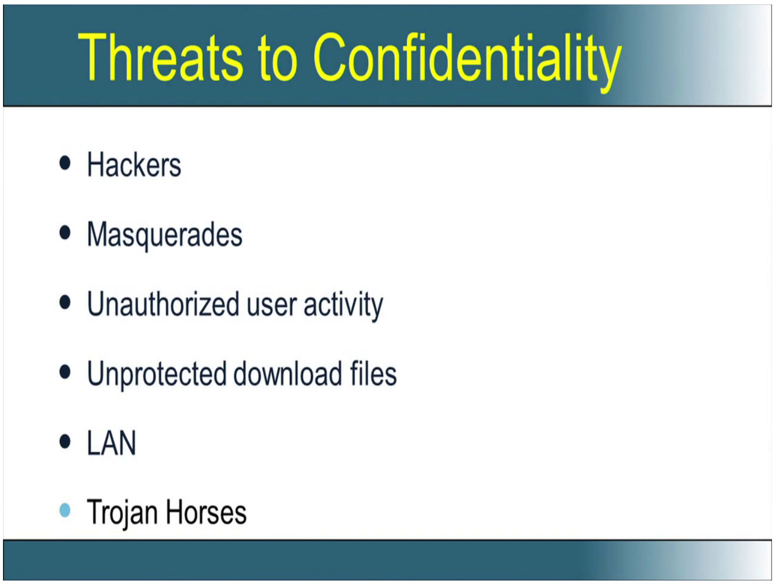
□ For how long is the protection needed?

First let us look at confidentiality. This in other words, in raw words it is called privacy. So, different questions come up when we just look at confidentiality. How do you go and define confidentiality? The definition of confidentiality comes from answering these three questions. What needs to be protected, how much protection is needed and for how long should we protect it? Whenever we look very interestingly on what needs to be protected, we say its personal information, its not just personal information. It can be privileged information, it could be business secrets. Interestingly it can also be geological or environmental information. So, what is so important about geological.

Recently, there was a newspaper article which said that a criminal actually hired a building that was close to half to 1 kilometer away from the bank, from a bank. He actually dug a tunnel from the empty house and dug the tunnel till the safety locker room of that bank, and he may go and able to break open the safety locker and get away with the jewels. So, this is essentially a geological information, an environmental information that there exists a house which is an old one and that one can dig a tunnel from that house close to half a kilometer and reach exactly a spot inside the bank in which the safety lockers are there, and then to get off. It is very important information about the bank, about the structure of the bank that was made available to the criminal. So, that information is essentially privileged information because the leaking out of that has really created a loss of wealth to the bank.

Ocean 11, Ocean 12, Ocean 13, these are series of movies. In one of the movies, they wanted to have an access to a very highly protected data center say 6-7 tiers of security, but they knew that when there is an earthquake, then some safety access controls systems inside the data center would not function. So, they actually used equipment, the criminals actually in that movie used equipment which will stimulate an earthquake and the access control system within the data center actually stops working for 6 minutes and within 6 minutes, they enter into the data center. So, there again is a very interesting example. Though it is a movie, it is a good example of geological information. So, even these informations are to be protected in the interest of the institution. The next question comes up is how much protection is needed and for how long is the protection needed?

(Refer Slide Time: 05:25)



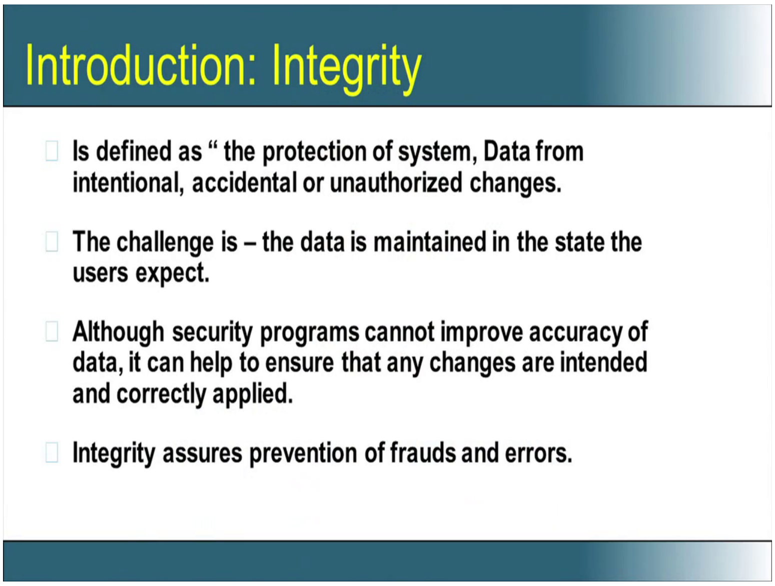
Threats to Confidentiality

- Hackers
- Masquerades
- Unauthorized user activity
- Unprotected download files
- LAN
- Trojan Horses

Now, let us look at the different tricks to confidentiality. A hacker, an user with malicious intent, an unauthorized user with a malicious intent is how you define a hacker. He is a threat to the confidentiality. The other thing is masquerading. I can mimic an authorized user, come into the system and steal information from the system. Any unauthorized user activity, he is a authorized user but he is doing an activity which he is not supposed to do, is also a threat to confidentiality, he is trying to access a file for which he doesn't have privileges. Unprotected download files. In one of the early lectures, I did mention about mega upload where people did upload files, but along with malware. So, these files when they are downloaded and you open them, so you install the malware in your system. If you go and ask the system who installed, it will say the user yourself has installed, but without your knowledge. And that malware can essentially steal information from your system.

Local area network itself is a threat to confidentiality because this is how the first exposure of a system to a neighboring system is through the local area network. So, securing the local area network itself is very important for maintaining confidentiality and of course, the Trojan horses. The Trojan horses are some back doors by which you can create, you can steal information. One very interesting example of a Trojan horse was that of a database which was a very popular database in which the back door of the trap was that in any installation if you enter the user name as politically and password as correct; it give an admin privilege to whoever enters this username and password. This was found after seven years of deployment of commercial versions of the database and it was a very very important vulnerability and it is Trojan which was done by the programmer. If you look at several millions of lines of codes, it is very difficult for somebody to actually find out that such as Trojan exist by inspecting a source code and this has led to vulnerability where some one gets an administrative privilege into a database by doing this. So, it is a very well quoted example of a Trojan horse.

(Refer Slide Time: 08:34)



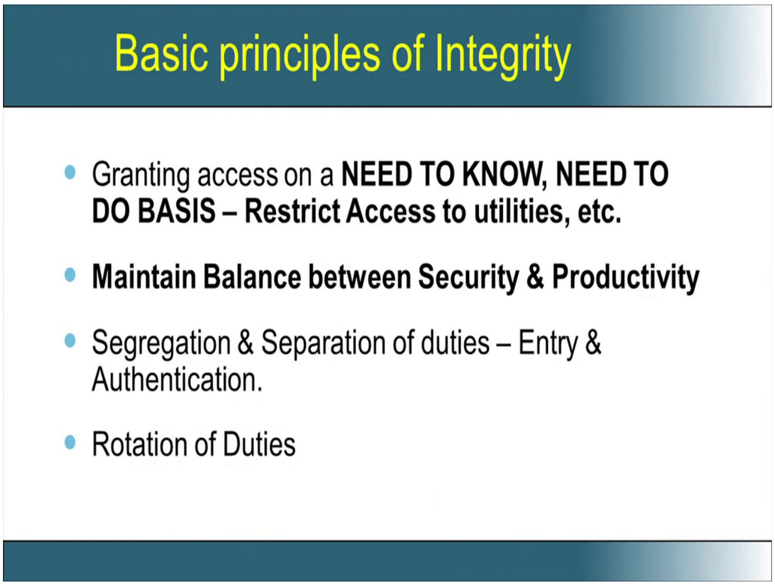
Introduction: Integrity

- Is defined as " the protection of system, Data from intentional, accidental or unauthorized changes.
- The challenge is – the data is maintained in the state the users expect.
- Although security programs cannot improve accuracy of data, it can help to ensure that any changes are intended and correctly applied.
- Integrity assures prevention of frauds and errors.

The next aspect, we have some idea about what is confidentiality. Now, we will go and look at the next aspect of the CIA which is integrity. What is integrity? I need some trust on the data. This data is correct, this data is accurate, this data has come from a known source, this data has come from a reliable source and I can rely on this data for its accuracy and authenticity. This type of feel is basically what we term as integrity. So, integrity is actually defined as the protection of the system, the data from intentional, accidental or unauthorized changes. The main challenge in integrity is the data should be maintained in the state the users expect it, they want. It is not the expectation, is not the value of the data. It is not just the value of the data; it is the format in which the data needs to be stored. It is also that the data should come from a reliable source; it is also that the data should not be accessed by unauthorized people. All these constitute this integrity and all these are what the users expect the data to be.

So, maintaining data is not the value, but also who access it, who can manipulate it. All this comes under data maintenance and that all dictates, that all defines the integrity of the data. Although many of the security programs cannot improve accuracy of data, but it can help to ensure that any changes to data are intended and correctly applied. The integrity assures prevention of frauds and errors.

(Refer Slide Time: 10:35)



Basic principles of Integrity

- Granting access on a **NEED TO KNOW, NEED TO DO BASIS – Restrict Access to utilities, etc.**
- **Maintain Balance between Security & Productivity**
- Segregation & Separation of duties – Entry & Authentication.
- Rotation of Duties

So, now what is the basic principles of integrity? How can I get this integrity? One of the fundamental principle is, two principles are need to know and need to do basis; an user when he enters the system, he necessarily need not know all the things about the system. For example, if I am a user, I need not know what the configuration of the system is. I need not know what the C-segment, a password is for example. I as an user need to know only my password and I should be able to access only my files, and I as a user, I need to do only some basic things. For example, I may not go and reconfigure or format a file system. As a user I am not supposed to go and format a file system. So, for every user there is something that he needs to know and there is something that he need to do for a given functionality.

Now, integrity can be ensured in a system if you go and make this policy rigorouson every user. You go and say this is what he needs to know and this is what he needs to do, he should not do something more than that, he should not know something more than that and this is something which will make your system, which will help you in a large way to maintain integrity of the information that is stored in your system. Now, when we are talking about integrity, we need to maintain balance between security and productivity.

So, when I try to go and say implement this need to know and need to do basis very rigorously, one of the thing is for example, I go inside that every one minute the person who is sitting in front of a console should give a finger print biometric base authentication that is indeed the person who is sitting. So, one cannot move from the system and some body else should not use the same system with the same log in and password. So, at every 30 seconds or 1 minute, I want every user to authenticate in the system we are sitting that they are indeed sitting using a biometric. Now, biometric will take several, at least some seconds to authenticate. So, what happens is this is a very rigorous security. So, in a one full day of say 9 hours of working time, this fellow will be authenticating for say 6 hours. So, every 30 seconds is going to spend say 10 to 15 seconds on authenticating himself. So, he will be doing more of authenticating himself rather than doing the work of the company. So, essentially if you start putting rigorous security measures, then your productivity essentially goes down. The other important thing which we will be discussing more details towards the end of this session is about segregation and separation of duties.

For example, let us talk about entry and authentication. I enter into a system using my user name and there is a password, and the password is done by the authentication. My password is authenticated. Now, who is going to allow me, who is going to give me the entry key? The sys admin creates the account. So, he is responsible for the entry and who authenticates. So, for the authentication we need a password. The password is set by the user. So, the duty of a system administrator is to give you a log in; the duty of the user to have a very strong password. So, there is certainly a segregation and separation of the duty of who is going to create the entry and who is going to create the authentication. So, this is one segregation we will talk more about this segregation as we proceed in this lecture. The next part is the rotation of duties.

(Refer Slide Time: 15:09)

Information
Assurance
Awareness
Program

LOCK IT UP when you leave

Information Protection

(Refer Slide Time: 15:11)

Information
Assurance
Awareness
Program

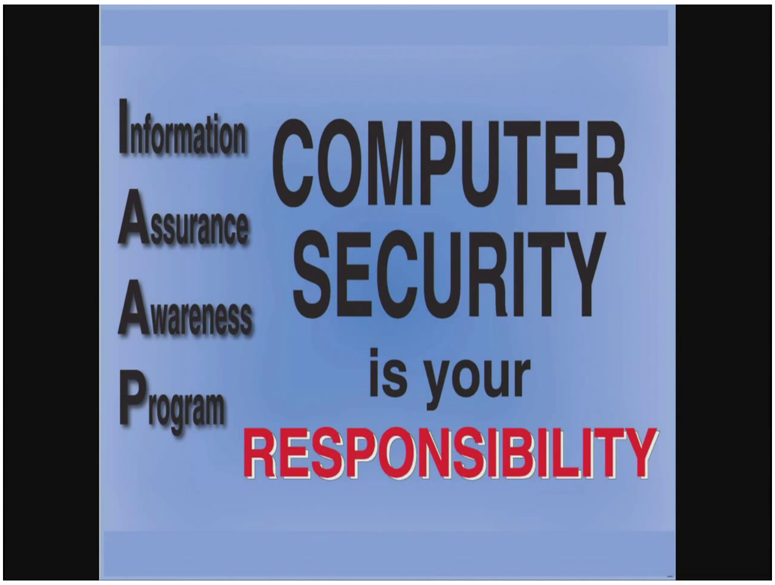
Copyright Laws apply to

- SOFTWARE
- SOUND BITES
- BOOK QUOTES
- GRAPHICS/CLIP ART
- PHOTOS
- VIDEO
- FONTS
- MP3s

Don't Hang us out On a Limb!

KEEP IT LEGAL

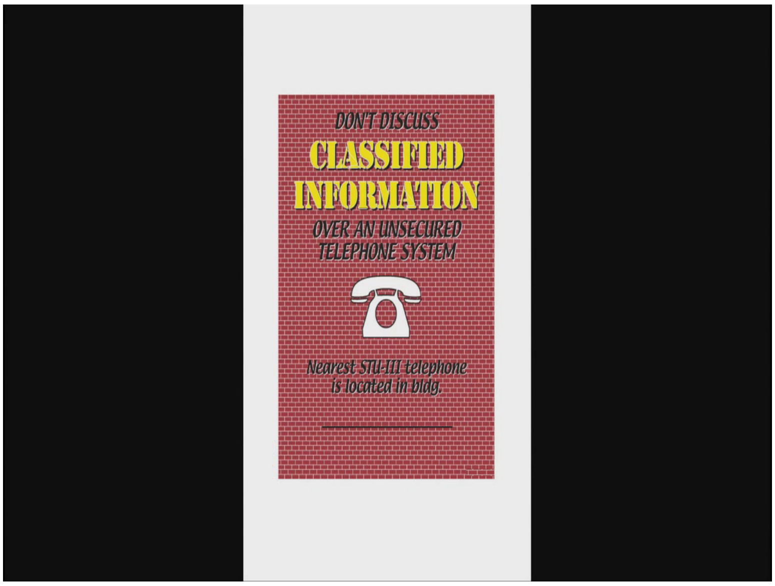
(Refer Slide Time: 15:16)



Information
Assurance
Awareness
Program

COMPUTER SECURITY is your RESPONSIBILITY

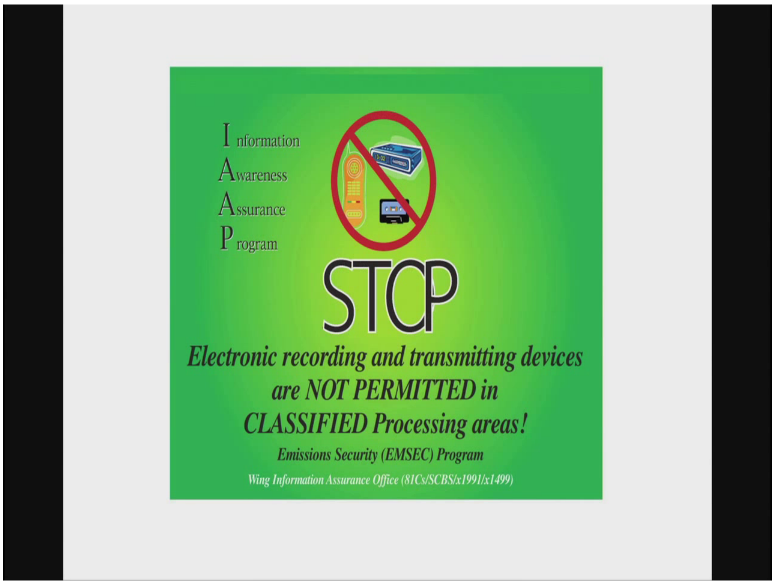
(Refer Slide Time: 12:21)



DON'T DISCUSS
CLASSIFIED INFORMATION
OVER AN UNSECURED TELEPHONE SYSTEM

Nearest STU-III telephone is located in bldg. ______________

(Refer Slide Time: 15:27)



I nformation
Awareness
Assurance
P rogram

STOP

Electronic recording and transmitting devices
are NOT PERMITTED in
CLASSIFIED Processing areas!

Emissions Security (EMSEC) Program

Wing Information Assurance Office (81Cs/SCBS/x1991/x1499)