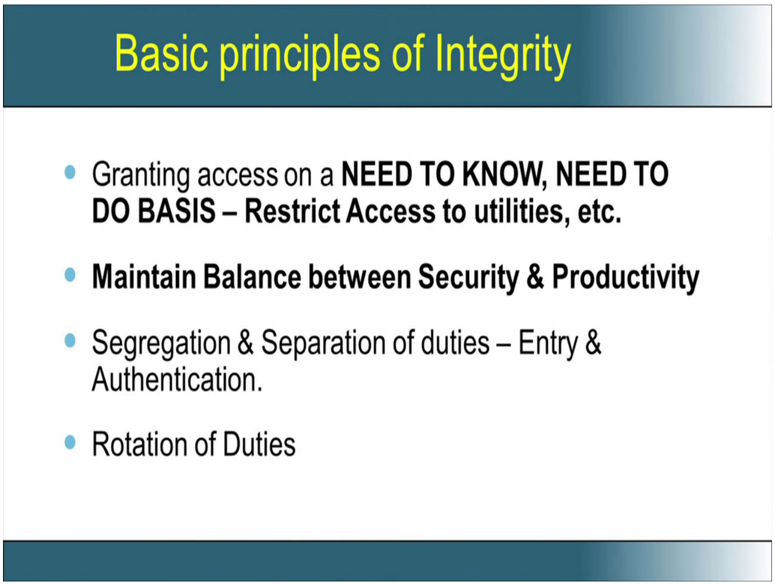
Introduction to Information Security

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

Lecture - 06

Rotation of duties means that the same person should not be involved in maintaining or doing some activity for long.

(Refer Slide Time: 00:02)



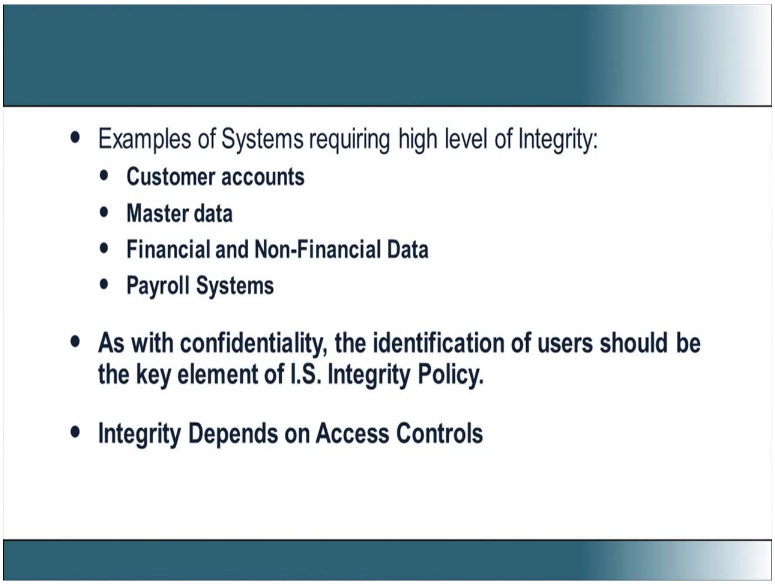
Basic principles of Integrity

- 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

This actually creates a good amount of redundancy within the system and at one point of time, if suppose I have a data and I don't know what the data is, no one in the organization knows what the data is except one person. Then, that person can essentially go and change the data in the way he wants, because no one can go and verify what that data means.

So, it is always important that many people come to know many things about many data, if that is not ensured then the organization will face the problem of what we call as, it is something like one fellow ownsthe data and nobody else knows about that data and so if, then he can go and change whatever format he wants and nobody can go and verify. So, rotation of duties ensure that this particular problem is addressed, it gives at least more than one people to have knowledge about every information asset that the company processes.

(Refer Slide Time: 01:35)

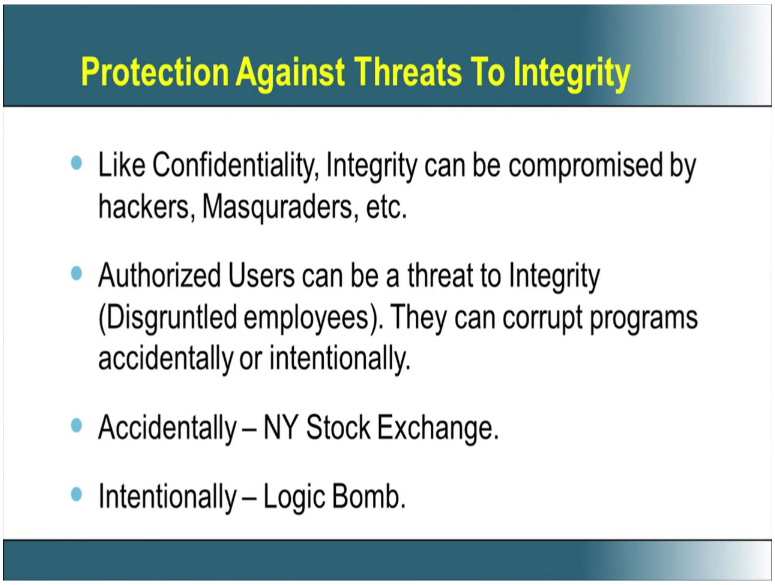


- Examples of Systems requiring high level of Integrity:
  - Customer accounts
  - Master data
  - Financial and Non-Financial Data
  - Payroll Systems
- As with confidentiality, the identification of users should be the key element of I.S. Integrity Policy.
- Integrity Depends on Access Controls

So, now let us look at some of the systems which require very high level of integrity. For example, the customer accounts is an information which needs to have high level of integrity. The master data, the financial and non financial data, the payroll systems all this needs to have very high level of integrity. As with confidentiality, the identification of users should be the key element of information security integrity policy. So, how do I go and ensure integrity, first thing is I need to identify the user.

So, how do we do this identification, again we have the process of identification, authentication and then we have what we call as the authorization, all that we did for the case of confidentiality needs to be done here. So, a user identifies himself through a login, then there is a password, then the authentication happens. Then, there is an authorization and based on this authorization, he can now go and do certain actions, do certain consistent actions on the data. So, what can an authenticated users do on different information assets inside the system, so that it is integrity will not be affected, it is basically dictated by the access controls. So, for us to ensure integrity, we need to have access controls. Now, we will look at different access controls that form that the basis of enforcing integrity.

(Refer Slide Time: 03:43)



Protection Against Threats To Integrity

- Like Confidentiality, Integrity can be compromised by hackers, Masquraders, etc.
- Authorized Users can be a threat to Integrity (Disgruntled employees). They can corrupt programs accidentally or intentionally.
- Accidentally – NY Stock Exchange.
- Intentionally – Logic Bomb.

When we look at protection against threatsthreat to integrity of course, like confidentiality, integrity can be compromised by hackers, Masquraders, etcetera. The authorized users can also be a threat to integrity. For I, they can go and corrupt programs accidentally or intentionally and that could cause integrity issues. I can give you a very simple example. In many servers there are certain configuration parameters which are set a boot time. So, when the system boots it reads the parameters and based on the parameters the server does some action and that parameter remains same, till you reboot the system again.

For example, there is a parameter a and I set it to a value 2, when the system boots it will read the parameters value as 2 and it will continue working. When the system is working when I go and change the parameter value to 3, nothing will happen to the system. But, when you shut down the system and reboot the system that time it will read that value as 3 and start doing something different.

So, let us take this type of scenario Now many of these servers have some parameters, if you set it to 1, it will share memory across applications. That means, your memory utilization becomes very good. If you set it as 0 then it does not share memory and then if you have very high memory intensive programs, then the server will essentially crash. Now, let us have one disgruntled employee who is maintaining the data centre, on the day when he sent out just before leaving, since still he has the authorization, he can get just go and change this memory sharing parameter from 0 to 1 or 1 to 0. Nothing will happen immediately, because it is a boot time parameter. After 5 or 6 months when the system boots up, it will read this parameter as 0 and then what will happen, the system will crash, it starts crashing and it will be very difficult for somebody to come and find out, this was because of the parameter change.

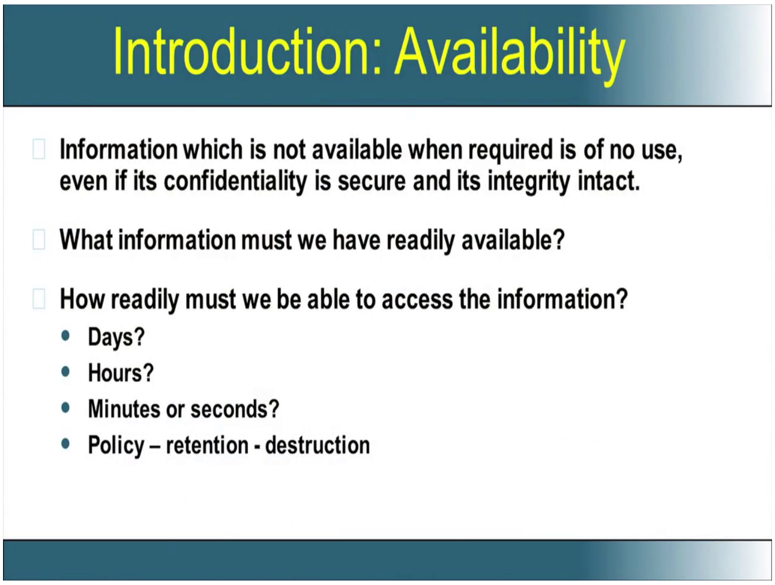
So, what has happened there was essentially an integrity issue here, where a configuration parameter has changed its value intentionally. So, the threat to integrity can also be within the system, it is not necessarily outside the system. So, there are two well quoted examples about threats to integrity. An accidental event which actually caused a threat to integrity was the New York stock exchange issue, where in somebody accidentally try to sell a huge number of stocks and that went and crashed down the servers and it create an availability issue and an integrity issue, it was a very accidental thing.

Similarly, one intentional case study that is well reported and well articulated in many information security literatures is the logic bomb. There is an employee who wrote a software for a company in which he said in case I am dismissed he wanted to create havocin the company. So, what he did was that on 7th of every month, if the software does not see his name in the payroll list, then he said go and delete all the files in the server, so he wrote the software like this.

So, on one fine month he was fired, the next month when 7th came, the software did check if his name was there in the payroll, his name was not there in the payroll and so it went and deleted everything in the system. So, this is an attack on the integrity, it is an intentional attack and that originated from within the system. This is commonly quoted as the logic bomb.

So, to sum up what we have seen so far is the definition of confidentiality and potential threats to confidentiality and how we can maintain confidentiality and we are also looking at integrity, we have seen different issues of integrity and how we can try and maintain integrity.

(Refer Slide Time: 08:42)



Introduction: Availability

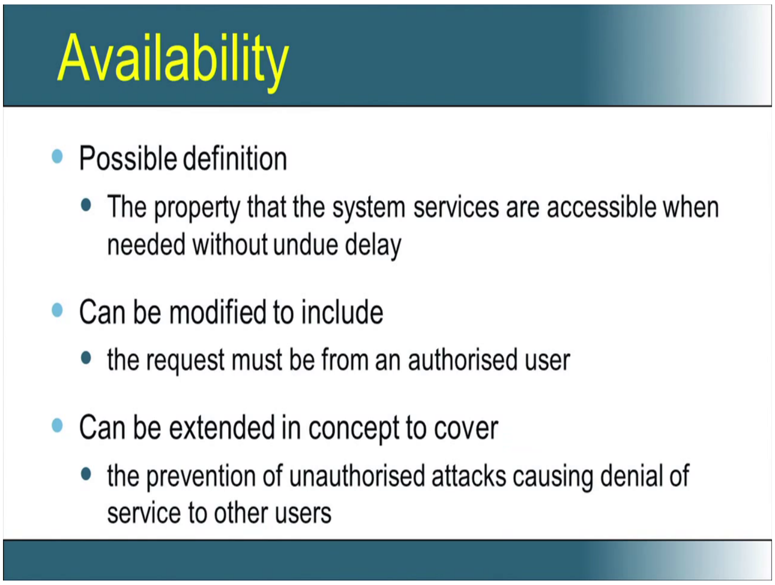
- Information which is not available when required is of no use, even if its confidentiality is secure and its integrity intact.
- What information must we have readily available?
- How readily must we be able to access the information?
  - Days?
  - Hours?
  - Minutes or seconds?
  - Policy – retention - destruction

Now, we go to the third point of availability. What is availability? So, we would like to come with a good definition of this, that the information should be available means, it should be available to an authorized user and it should be available in the form that is needed by the user. The user wants to maintain some format, he needs some integrity, confidentiality, etcetera and so and this data should be made available within some fixed amount of time.

So, all these things are involved when we try to define what is availability? So, the information which is not available, when required is of no use. Even if you say I have got the highest degree of confidentiality and integrity, this information is of no use. So, the question now comes what are the information that must be made readily available.

So, that forms one of the important ingredients of your security policy, what is said that I should make it available and how readily I should make it available, should it be in days, hours, minutes or seconds. How much time should I maintain the data, should I backup the data, when can I destruct the data, all these things come as a part of yourinformation security policy.

(Refer Slide Time: 10:19)



Availability

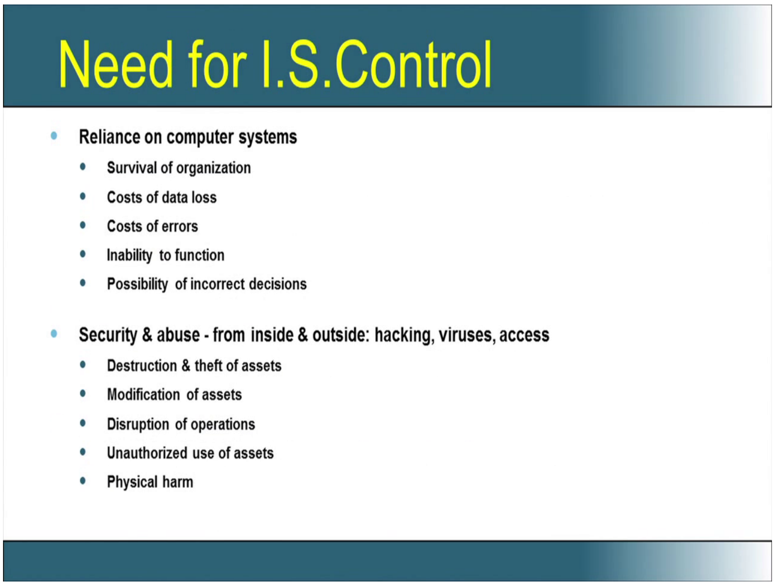
- Possible definition
  - The property that the system services are accessible when needed without undue delay
- Can be modified to include
  - the request must be from an authorised user
- Can be extended in concept to cover
  - the prevention of unauthorised attacks causing denial of service to other users

So, with this as a background we will go and start defining availability. So, availability as you see is the property that the system services areaccessible when needed without undue delay. As said what is data that should be available, first data is the system services, first information I said is the system services, they should be accessible when needed without undue delay. And with some more of what we saw in the previous slide, we can say that the system services when it is requested by an authorized user should be available without undue delay. And we can also go and add say the second facet of this definition, where we need to prevent unauthorized attacks causing denial of services to other users. So, availability means for an authorized user, the system services the information assets should be accessible when needed without undue delay and prevention of unauthorized attacks which can cause denial of service to other users.

So, we have been using this word denial of services, what you mean by a denial of service. For example, I have several computers within a office which are connected through a network. Now, when one computer wants to talk to another computer, it is start using the network. Note that this network is a shared resource, if I am going to increase that traffic on a network, traffic means the amount of data transmitted on the network, beyond some threshold then what would happen, the network will choke and because of this choking what will happen, a computer A cannot talk to computer B, this means that there is an availability issue and this is a security issue, because we are not giving the availability of this.

Now, how can I create the traffic, there can be another system within the local area network who starts sending arbitrary packets on the network which will go and choke the switch, the network equipment. And so, the network equipment will be very busy handling these packets which are coming from this unauthorized source. And so the amount of attention that network device can give for the communication between computer A and computer B essentially decreases. So, the response time between computer A and computer B, the response of computer B as perceived by computer A and the response of computer A as perceived by computer B will not be as per the expectation and this is actually called denial of service. The denial of service with respect to your particular system is completely external to the system, but it can stop this system from communicating to the neighbouring systems and do an activity. So, this is one example of a denial of service. We will talk about many examples of denial of service as we proceed through this lecture.

(Refer Slide Time: 13:50)



Need for I.S.Control

- Reliance on computer systems
  - Survival of organization
  - Costs of data loss
  - Costs of errors
  - Inability to function
  - Possibility of incorrect decisions
- Security & abuse - from inside & outside: hacking, viruses, access
  - Destruction & theft of assets
  - Modification of assets
  - Disruption of operations
  - Unauthorized use of assets
  - Physical harm

Now, what we need is we need to get this confidentiality, integrity and availability in the system and how do we get this, we need to impose some control and this is called information security control. For need to ensure confidentiality, integrity and availability I need to put certain control mechanisms inside the system which will basically ensure this. Why do we need this control? This control becomes extremely important, because we are using computers today for survival of many organizations.

If the computers don't exist, if the computers are compromised, the organizations cannot survive and if I do not have proper information control I will have data loss and the loss of data is very, very costly. I would have errors again the cost for these errors should be extremely high. And I may not be there could be a denial of service I cannot even function and because of this wrong data as I mentioned earlier, the data is used for making business decisions and if I go and corrupt the data, then I could possibly make incorrect decisions which can hamper the growth of the organization.

If I don't have control, then what will happen is there could be an abuse from both inside the system and outside the system through things like hacking, viruses, unauthorized accesses, etcetera. And the moment my system is abused, now all my information asset either can be destructed or they can be stolen, they could be modified, my operations can be disrupted, I could have unauthorized use of my assets and I can also have physical harm, the system can get burnt.

So, all these things can basically go and it is a potential threat to the survival of the organization. Because, now we are talking of more and more reilance on computer systems, information security based control becomes inevitable, we have to have such type of controls and these controls in place, we can basically talk of confidentiality, integrity and availability as our security goals. Now, we will go and look at what are all the controls.

(Refer Slide Time: 16:37)

What are Controls???

"Controls are defined as Policies, Procedures, Practices and organizational structures (Administrative Control) designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected (Technical Control)"

COBIT

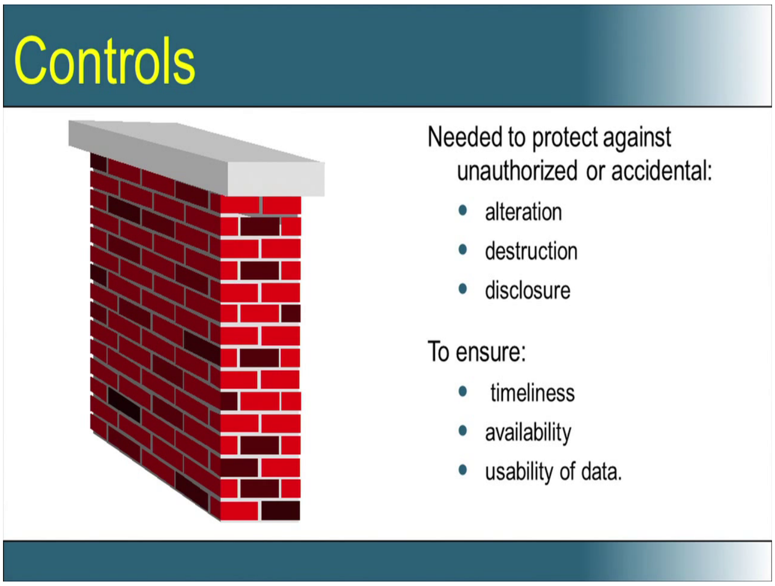
So, control is of two types, one is dictated by the administration, another is technical. Now, COBIT actually an organization, COBIT is a standard, it comes out with the definition of control. Controls are actually defined as policies, information security policies, procedures that implement these policies, practices that comes out due to the procedures and the different organizational structures that are in place to maintain this policies, procedures and practices.

So, controls are defined as these policies, procedures, practices and organizational structures which are designed to provide reasonable assurance that the business objectives will be achieved and that undesired events will be prevented or detected and corrected.

So, the policies, procedures, practices and organizational structures form the part of the administrative control and once those things are in place now to ensure that no undesired events, undesired in the sense events that are prohibited by the policy that are not stated in the policy, that are not part of any procedures or practice, thus type of undesired events will be either prevented or if it happens, it should be detected and subsequently corrected.

The technical control takes care of stopping these undesired events, while the administrative control defines what are desired events and what are undesired events. So, control when we look at from the broad perspective is a combination of administrative and technical control. We will now talk more about this control as we proceed.

(Refer Slide Time: 18:46)



Controls

Needed to protect against unauthorized or accidental:

- alteration
- destruction
- disclosure

To ensure:

- timeliness
- availability
- usability of data.

Now, what do we want to control, what is the goal of control? The goal of control is to maintain the CIA. Now, let us look at the negation of this, it is to protect the system from what we call as DAD, C is confidentiality, the opposite of confidentiality is disclosure, I is integrity, the opposite of integrity is alteration, D is availability the opposite of availability is destruction. So, I need control to maintain CIA, it is essentially to mean I need controls to protect the system from disclosure, alteration and destruction.

So, the control can also be defined in this form, so I need control to prevent or protect a system from disclosure, alteration and destruction and to ensure that any services is available within a prescribe time limit and the data is in a usable format or the information is in the usable format. So, this is how I can define the role of control in an information security framework.