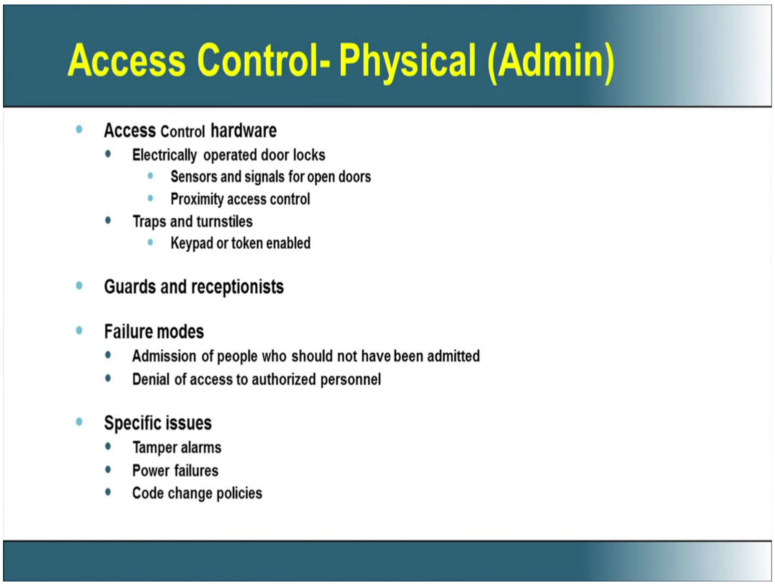
Introduction to Information Security
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 08 So, as I have mentioned control is very important for ensuring CIA and protect the system from DAD that is Disclosure Destruction Alteration.

(Refer Slide Time: 00:09)



Access Control- Physical (Admin)

- Access Control hardware
  - Electrically operated door locks
    - Sensors and signals for open doors
    - Proximity access control
  - Traps and turnstiles
    - Keypad or token enabled
- Guards and receptionists
- Failure modes
  - Admission of people who should not have been admitted
  - Denial of access to authorized personnel
- Specific issues
  - Tamper alarms
  - Power failures
  - Code change policies

So, the notion now that we have been talking of two types of controls one is the technical control and the administrative control. One of the important administrative control that should be a part of information security document is the access control, physical access control to the building that houses the data centre. So, the data centre can have electrically operator door locks which has sensors and signals for open doors, they have proximity access control, they could have traps and turn styles to stop piggy bagging.

So, for every biometry based entry into the building, only one person can enter not many, they could have well trained guards and receptionists, all these are part of your access control. Now, what you mean by training a receptionist, so there is we has particular policy that should be followed when a new person enters the organization. If he is going to be a new employee there should be certain protocols followed, if he is going to be a guest, if he is going to be a technical visitor, he is going to be a visitor, visiting a friend, so there are different classes of people will come to a company.

So, how to handle them is what you need to train and these should all be the part of your information security policy. And the most important thing is if this fails like what do you mean by failure of an access control, an unauthorized person has entered or an authorized person is denied access, both of these are wrong. And so one of the important thing is how do we handle such type of a contingency situation. That should also be part of the information security document.

Then, there are specific issues here, if something undue had happens, something that should not happen has happened then there should be alarms. For example, tamper alarms. Somebody tries to break open the door or somebody tries to break open a biometry device or any access control device, then there is a power failure what would happen and suddenly there are some change in the code from... So, some companies give some blue badge, green badge, yellow badge, so a green badge cannot enter a gym for example, inside the company, it is only for employees and green badge can be a consultant.

So, tomorrow there is one a change that consultants also can enter the gym, for example. Now, these code change policies has to be quickly you know integrated into this access control systems. So, these are all the things that we need to keep in mind when we devise a physical access control system, this is for entry into the building or entry into different parts of the physical entry of a human being in to different parts of the building.

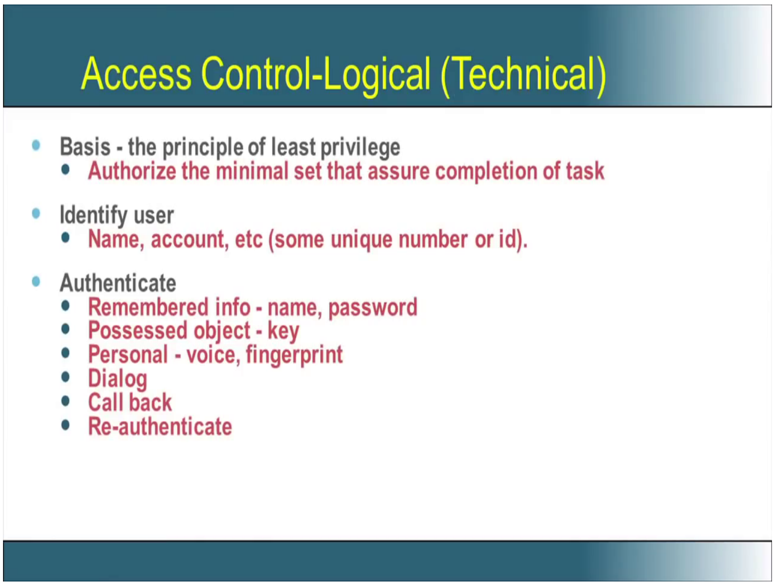
(Refer Slide Time: 04:09)

Technical Control

- Looked so far at Administrative Controls.
- Next we shall look at Technical or Logical Control

So far we have looks at different administrative control like physical access and the segregation of duties, next we shall look at little more of technical or logical control.

(Refer Slide Time: 04:24)



Access Control-Logical (Technical)

- Basis - the principle of least privilege
  - Authorize the minimal set that assure completion of task
- Identify user
  - Name, account, etc (some unique number or id).
- Authenticate
  - Remembered info - name, password
  - Possessed object - key
  - Personal - voice, fingerprint
  - Dialog
  - Call back
  - Re-authenticate

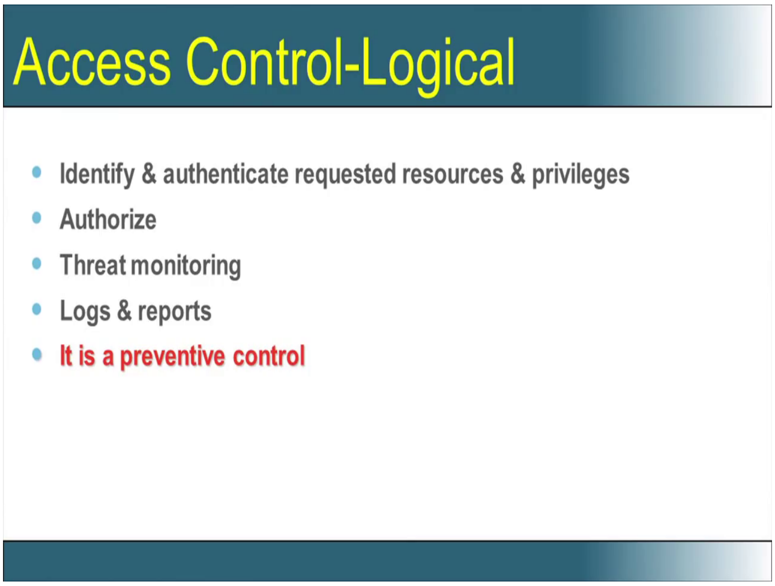
So, accessing a building through a security mechanism is a access control which is administrative. Logging into a system is again an access control, you are entering a system, but that is a technical access control, just to give you a distinction between technical and administrative. Now, when we talk of access control we have already talked of the basic things like identification, authentication and authorization.

Now, identification and authentication are the most important aspect of access control. So, how do you identify a user by his name or in some account or some unique number or id can be also an employee id and then how do you authenticate, there are several ways of authentication. It can be a name or a password, it is a remember information. It can be some key or a button he possesses, an object that the employee posses.

It can be a personal feature like a voice or a finger print, it also be through a dialog what is your pets name, what is your father's name you can be a callback, it can be a re authenticating. So, authentication can be done in many ways one or more of these ways, but one of the basic principles again we go back to what we discussed when we are discussing integrity is that when we authenticate this an user, the next thing comes the authorization, that authorization should be for the minimal set that assure completion of a task.

I as an user come into a system to do a task, for doing that task I need some minimal set of privileges and this authorization should give me only that minimal set of privileges, you should not give me more privilege than what I need to get as a user.

(Refer Slide Time: 06:45)



Access Control-Logical

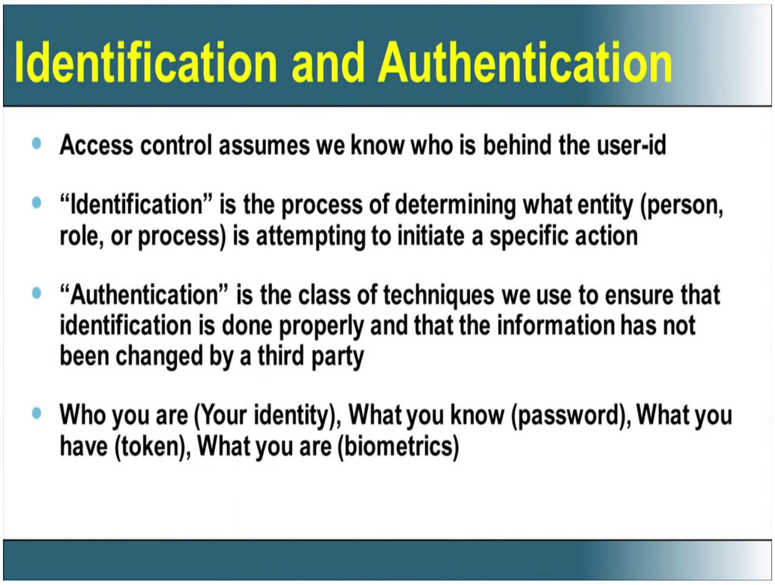
- Identify & authenticate requested resources & privileges
- Authorize
- Threat monitoring
- Logs & reports
- It is a preventive control

So, we identify and authenticate a user who request for some resource and privileges, we authorize the user for going and using these resources and privileges. When you authorize these users, one of the most important thing is to go and monitor some threats. The threat monitoring comes, we will be talking about that in subsequent modules in greater details, but the threat monitoring essentially is made possible by having logs and reports.

For example, a user logs in with many times with wrong password, there are many attempts to log into the system with different passwords and these passwords are different from each other much different. For example, one might be say Kamakodi with suppose I made A as capital and my password is Kamakodi, next time I make M as capital and I try this is not two different, but suppose I say Kamakodi and next time I say Dilip then these two passwords are very different.

So, I need to monitor this type and where do we get these details, we look at logs, we look at reports. So, there is the constant monitoring and auditing of the logs and reports, we cannot say auditing, more of monitoring of these logs and reports which will go and find that threat at the earliest possible time and stop that threat from penetrative. So, essentially it is a preventive control rather than allowing the system to exposing the system to threat and then trying to solve the problem by detecting and correcting. We now prevent the threat from entering and that is what access control does from a logical perspective from a technical perspective.

(Refer Slide Time: 08:46)



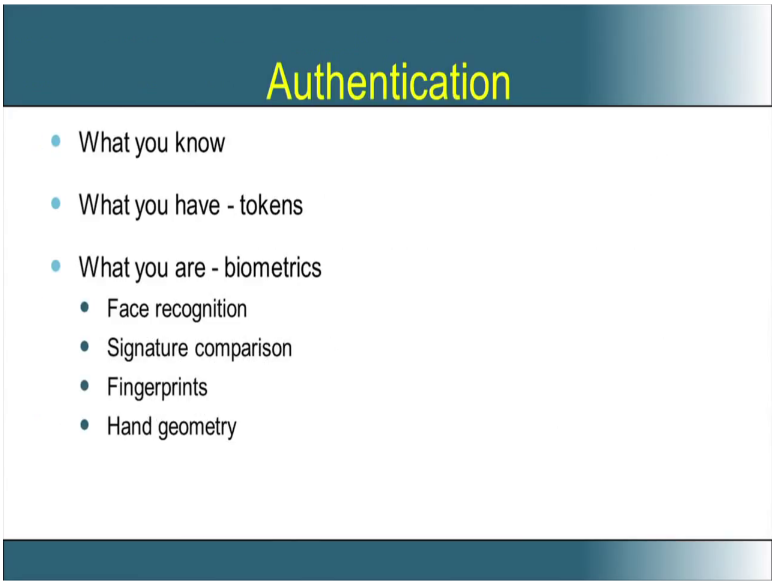
Identification and Authentication

- Access control assumes we know who is behind the user-id
- "Identification" is the process of determining what entity (person, role, or process) is attempting to initiate a specific action
- "Authentication" is the class of techniques we use to ensure that identification is done properly and that the information has not been changed by a third party
- Who you are (Your identity), What you know (password), What you have (token), What you are (biometrics)

We have talked about identification and authentication several times. But, I believe that I need to repeat it, I will be repeating it a little more time, because they really form the basis, now what is this entire process. So, we can neatly summarize with some beautiful questions, who you are, is the identification, what you know, what you have and what you are can be the authentication.

For example, who you are, is your user name, what you know, password or what you have, faithfully a token or what you are, a biometric way of iris can make the authentication. So, these four questions who you are, what you know, what you have and what you are can essentially solves the I and A requirement, I and A means your Identification and Authentication.

(Refer Slide Time: 09:48)

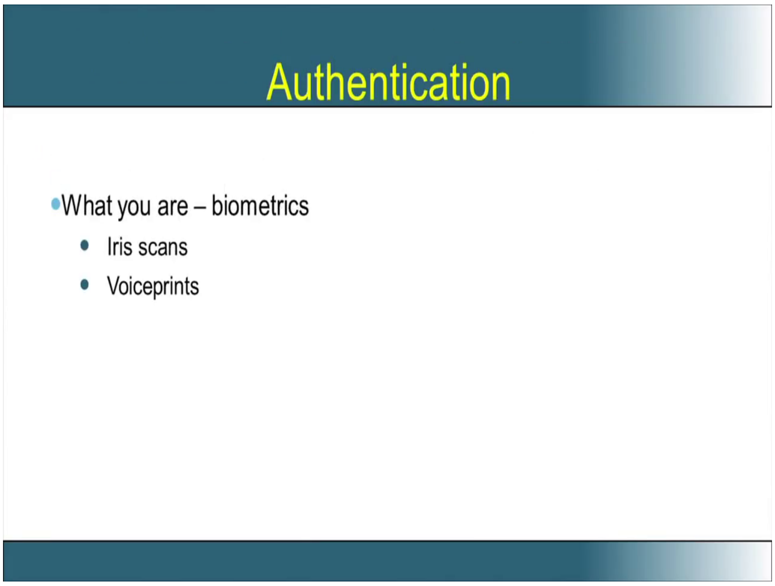


Authentication

- What you know
- What you have - tokens
- What you are - biometrics
  - Face recognition
  - Signature comparison
  - Fingerprints
  - Hand geometry

Now, when it comes to authentication what you are is very, very important, you have face recognition and you have signature comparison, you can have fingerprints, you can have hand geometry, you could have iris scan, you could have voice prints and all this form the basics of authentication.

(Refer Slide Time: 10:05)



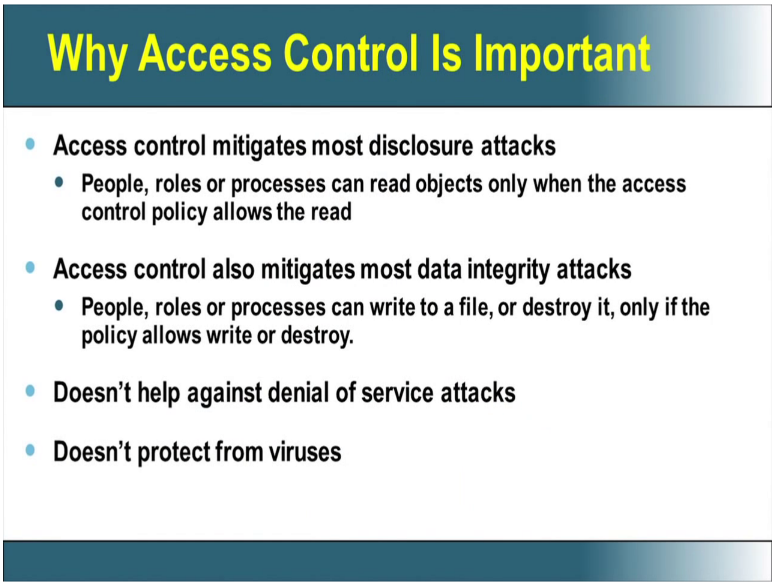
Authentication

- What you are – biometrics
  - Iris scans
  - Voiceprints

Now, suppose I go and say I will have all these authentications. So, for somebody to login to the system, he needs to have a password, then he needs to have a token, then his face has to be recognized, his signature has to be compared, his fingerprint has to be match, his hand geometry should match, his iris should match, his voice should be there. So, one day he has a bad throat, he cannot even enter the system. If suppose I have all these things then the whole day, half a day everybody will be trying to log in to your system.

So, I again come back to that point that there is a balance between security and productivity. If I over do on the security, then your employee will be spending half a day just to authenticate himself that he is him and so the system permits him to work on it. So, I just want to emphasize this point here, because there are different ways, there are different answers in the modern world about what you are that is biometrics. And so there should be a very clear balance between security and you know and the productivity. So, one of thesecan certainly be taken as an authentication machine.

(Refer Slide Time: 11:34)



Why Access Control Is Important

- Access control mitigates most disclosure attacks
  - People, roles or processes can read objects only when the access control policy allows the read
- Access control also mitigates most data integrity attacks
  - People, roles or processes can write to a file, or destroy it, only if the policy allows write or destroy.
- Doesn't help against denial of service attacks
- Doesn't protect from viruses

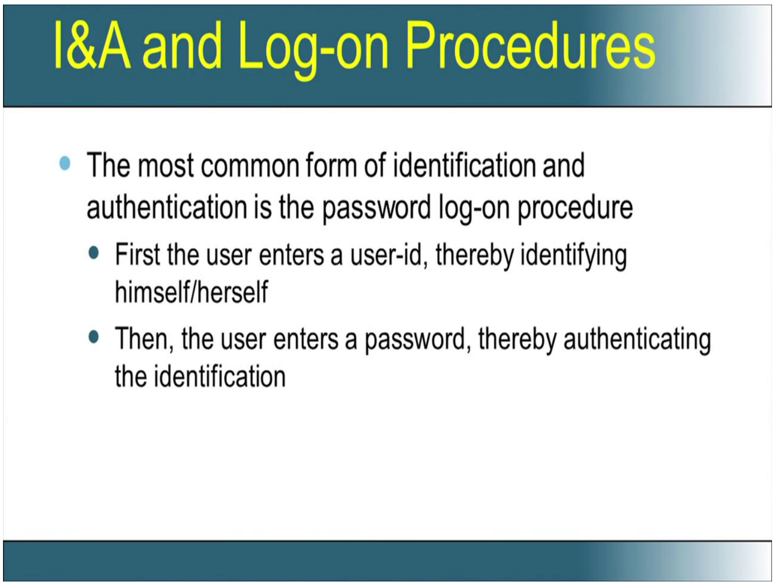
Now, why access control is important, we have already seen many of these, but logical access control here essentially means the logical access control, the technical access control essentially fixes for every person, his role and the processes that can permit him to read or for that role, what are all the processes that is accessible to him and what each of these processes can do. So, without this access control it would be very, very difficult for an organization to fix a clear role with clear authorization for a particular person.

So, if I have this access control if that means I could put a clear role for a person, I could fix a role for a person and I could give the necessary authorization that means I can mitigate many of the disclosure attacks, I can also mitigate many of the data integrity attacks. So, my information can be confidential, my integrity of the information can be maintained.

Of course, access control cannot ensure something like availability, it does not help like say my login and password and authorization that I have on a system cannot stop some other system from clogging the network and making some service unavailable to me. Your access control will not protect you from viruses. So, your access control is more or less internal to you and the system and it does not stop some external thing which is outside you to come and affect the system and hence create some security issues.

So, this understanding should be there, so when I am creating a system where I am ensuring the CIA, the C and I can come out of control. But, for dealing with A, it is not the access control, but you need some different type of control to make things available which you will be seeing down the line in great detail.

(Refer Slide Time: 13:56)



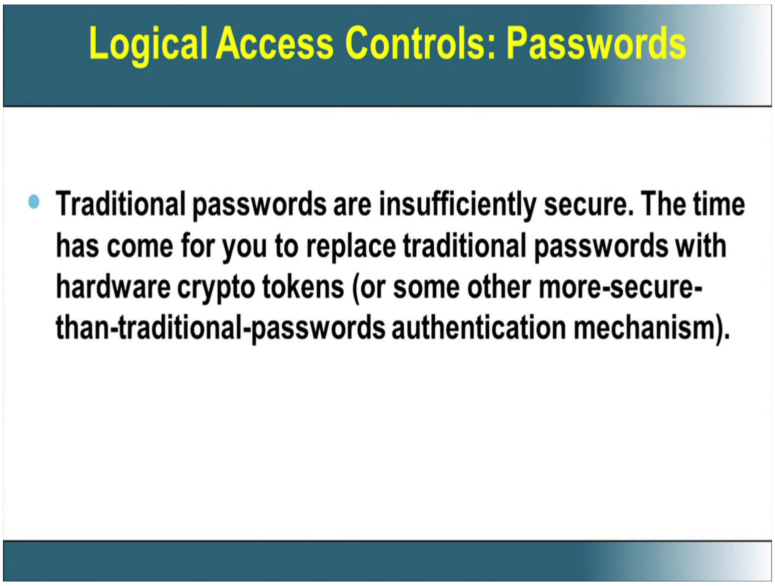
I&A and Log-on Procedures

- The most common form of identification and authentication is the password log-on procedure
  - First the user enters a user-id, thereby identifying himself/herself
  - Then, the user enters a password, thereby authenticating the identification

So, this is the general I and A procedure, today what is that, that is used in common today. You may have several login accounts on Gmail and Yahoo, your internet banking, your credit card. So, you will have several login and for professors, you may have different journals, you would have login and password, you would have several login passwords combinations.

But, you have any thing where we are using anything other than this password, probably in banks you may have a two steps or two or three step authentication, where they may send you an OTP, you may have two different passwords, but everything is password, one time password, a transaction password, a login password, so everything is password here.

(Refer Slide Time: 14:55)



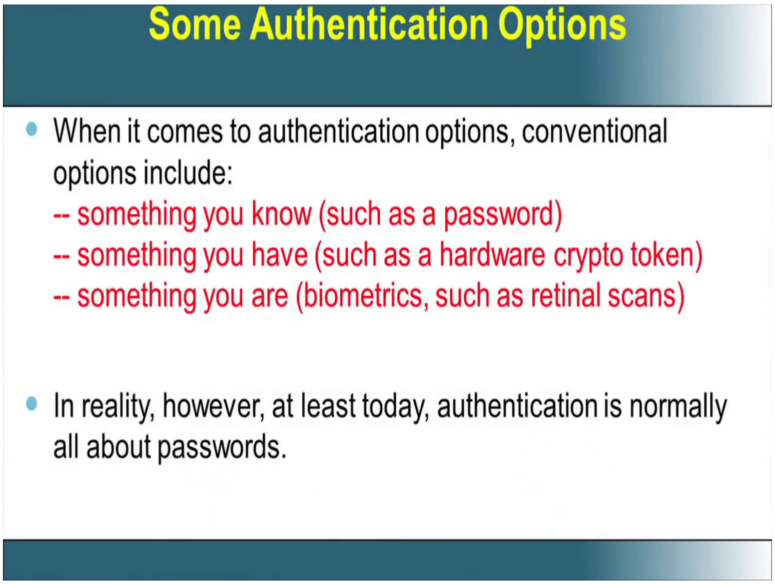
Logical Access Controls: Passwords

- Traditional passwords are insufficiently secure. The time has come for you to replace traditional passwords with hardware crypto tokens (or some other more-secure-than-traditional-passwords authentication mechanism).

So, now one of the thing that we will also see with some justification that traditional passwords are insufficiently secure. Now, people do have hardware crypto-tokens which are more secure than traditional passwords. What is a hardware crypto-token, it someone device which will be generating random numbers, let us say every 15 seconds and this device should be synced with the similar random number on your server. So, when I login form a remote client on to the server, I type this number and the same number if the number matches, then your login is true.

So, this is what we call as an hardware crypto-token and so it since that the password is changing dynamically, even if somebody guesses, it will be valid only for 15 seconds next time he can't login.

(Refer Slide Time: 15:54)



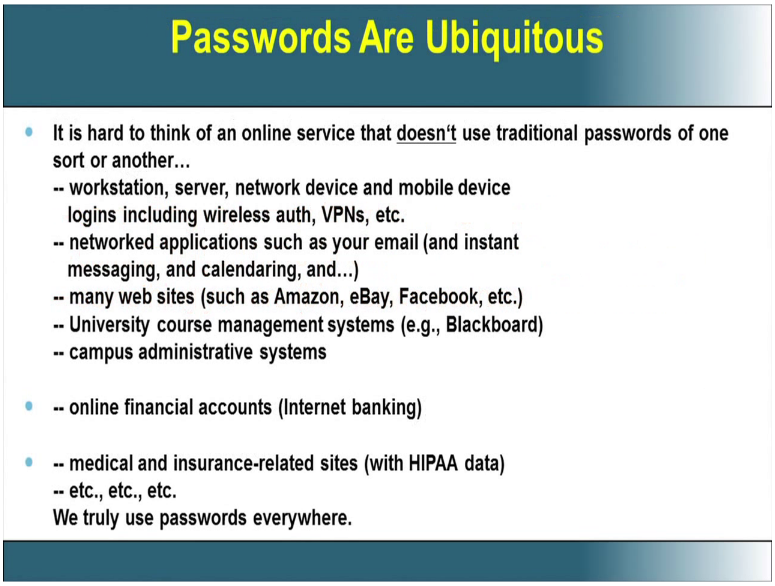
Some Authentication Options

- When it comes to authentication options, conventional options include:
  -- something you know (such as a password)
  -- something you have (such as a hardware crypto token)
  -- something you are (biometrics, such as retinal scans)

- In reality, however, at least today, authentication is normally all about passwords.

So, when it comes to such type of authentication option, the conventional options are something you know password, something you have hardware, something you have biometrics, such as retinal scans you have all these things. But, in reality however till today the authentication is normally all about passwords.

(Refer Slide Time: 16:18)



Passwords Are Ubiquitous

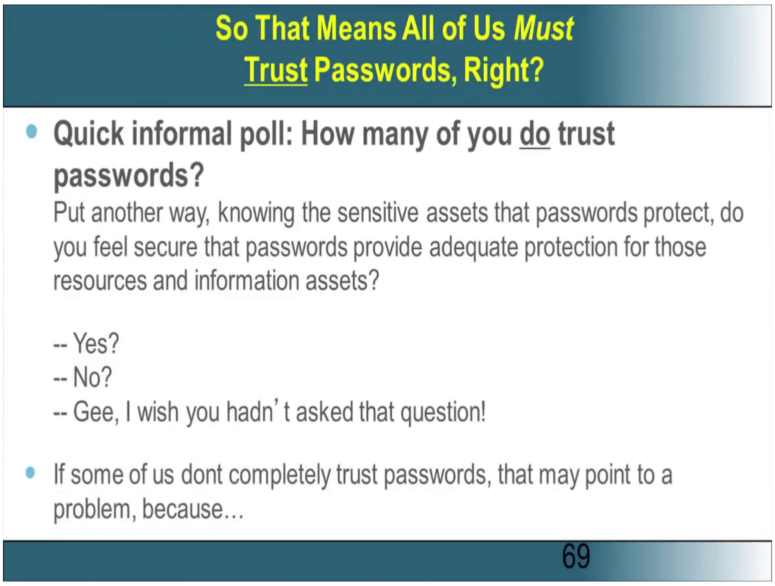
- It is hard to think of an online service that doesn't use traditional passwords of one sort or another...
  -- workstation, server, network device and mobile device logins including wireless auth, VPNs, etc.
  -- networked applications such as your email (and instant messaging, and calendaring, and...)
  -- many web sites (such as Amazon, eBay, Facebook, etc.)
  -- University course management systems (e.g., Blackboard)
  -- campus administrative systems

- -- online financial accounts (Internet banking)

- -- medical and insurance-related sites (with HIPAA data)
  -- etc., etc., etc.
  We truly use passwords everywhere.

Passwords are everywhere you go to workstations, you go to network applications, your email, your many websites like Amazon, eBay as I mentioned, your university course management system, your campus administration systems, your internet banking, your medical and insurance related things, the HIPAA is actually a medical standard. So everywhere we truly use passwords. It is ubiquitous.

(Refer Slide Time: 16:44)



So That Means All of Us *Must* Trust Passwords, Right?

- **Quick informal poll: How many of you do trust passwords?**

  Put another way, knowing the sensitive assets that passwords protect, do you feel secure that passwords provide adequate protection for those resources and information assets?

  -- Yes?
  -- No?
  -- Gee, I wish you hadn’t asked that question!

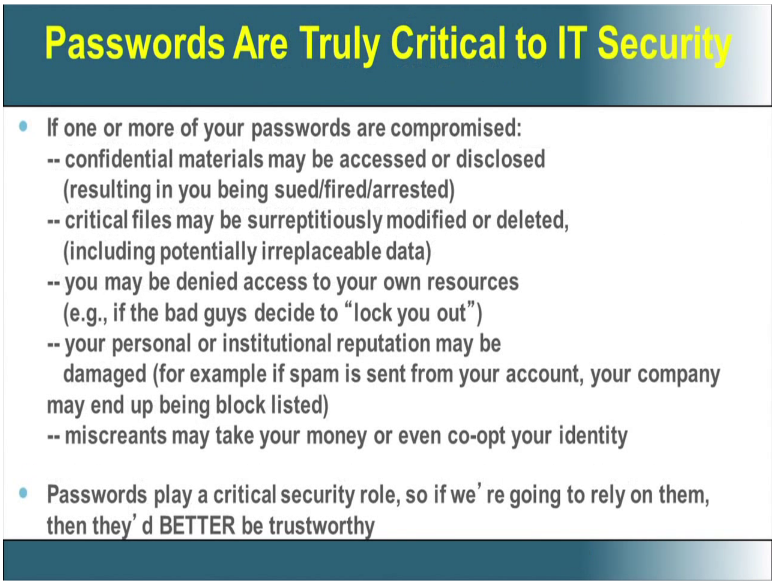
- If some of us dont completely trust passwords, that may point to a problem, because…

69

So, that means all of us must trust the passwords, so if we call a meeting of all and ask how many people trust password. Do you trust a password? Suppose, if you say no, you do not trust passwords that may point to a problem, because you cannot use any server many, many all many things that you have today uses only passwords.

So, you may not be in a position to use any service that is available, any information secure, information technology service, IT services that are available. So, the best answer today is I wish you hadn't ask the question. So, how many of us do trust passwords, though we do not trust, we do not have a go, we go and use it.

(Refer Slide Time: 17:38)

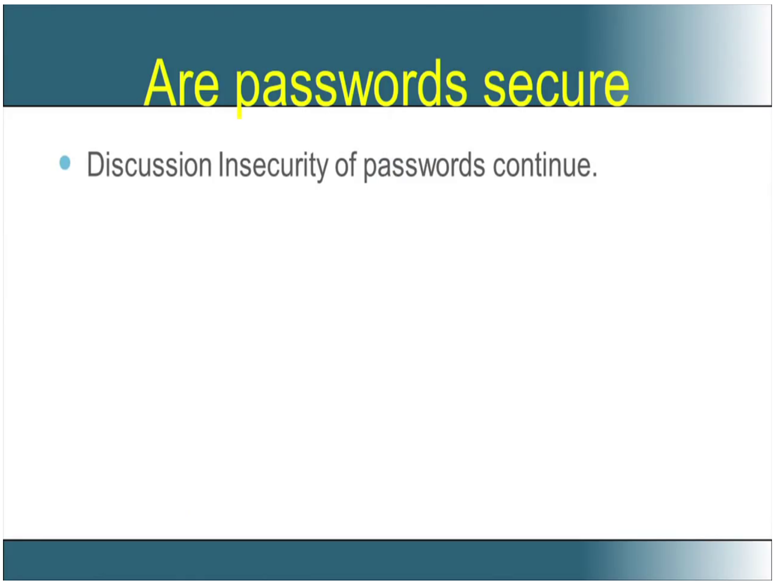


Passwords Are Truly Critical to IT Security

- If one or more of your passwords are compromised:
  -- confidential materials may be accessed or disclosed
  (resulting in you being sued/fired/arrested)
  -- critical files may be surreptitiously modified or deleted,
  (including potentially irreplaceable data)
  -- you may be denied access to your own resources
  (e.g., if the bad guys decide to "lock you out")
  -- your personal or institutional reputation may be
  damaged (for example if spam is sent from your account, your company
  may end up being block listed)
  -- miscreants may take your money or even co-opt your identity
- Passwords play a critical security role, so if we' re going to rely on them, then they' d BETTER be trustworthy

If one or more of your passwords are compromised, then what happens, all your confidential materials may be accessed, your critical files may be modified, you may be denied access to your own resources, somebody can go and change the password and also your secondary E-mail. So, there is no way by which you can recover, your personal or institutional reputation may be damaged. For example, they may send a spam or they can send a very nasty E-mail to your boss. And miscreants can also take your money or even co-opt your identity. So, passwords actually play a very critical security role, so if you are going to rely on them, then they better be trust worthy.

(Refer Slide Time: 18:27)



Are passwords secure

- Discussion Insecurity of passwords continue.

Now what we now do is arepasswords really secure and this is a very important discussion and we will discuss on the insecurity of passwords in the coming session.

Thank you.