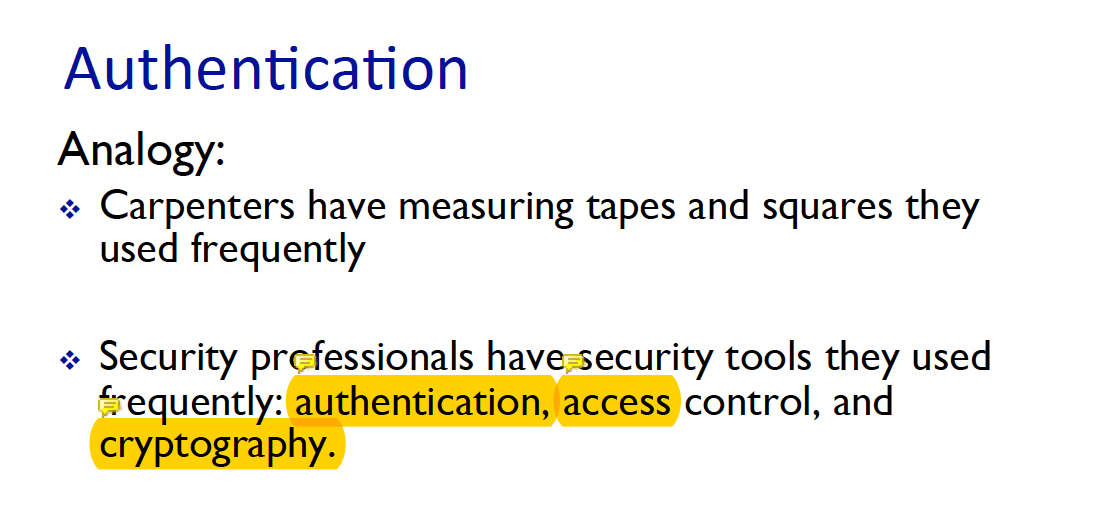
|  |  |  |
| --- | --- | --- |
|  |  | CPS 633 – note questions  Jae Duk Seo |

# Lecture 2 – intro to security

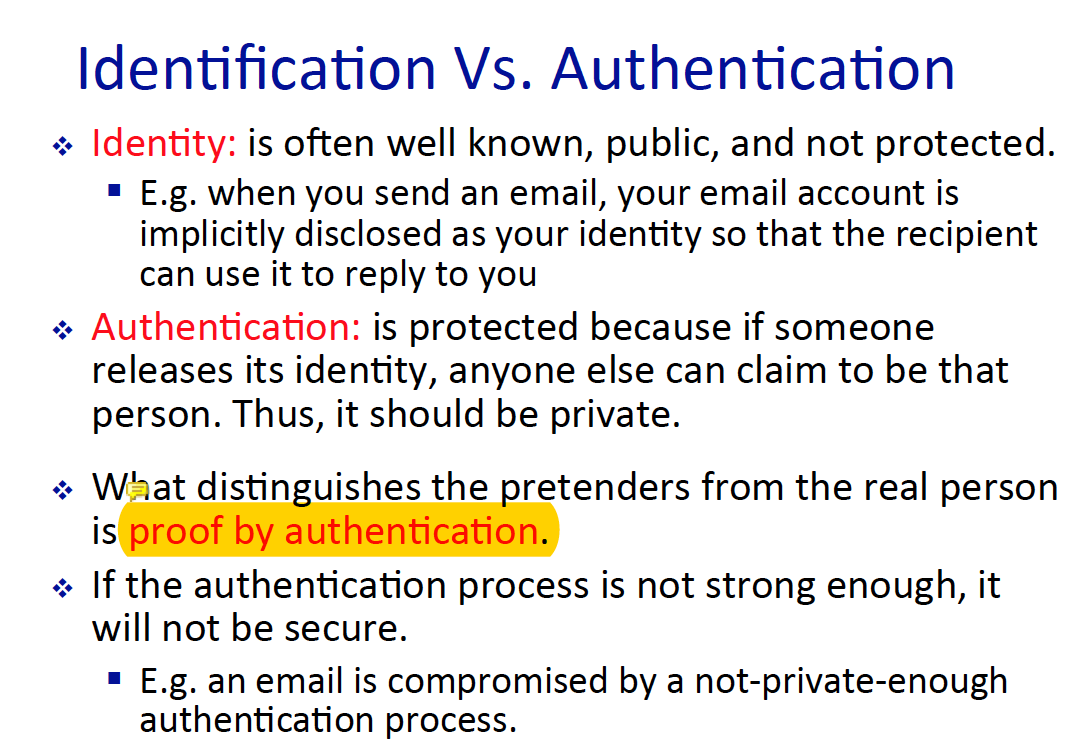
1. What are the tools for security professionals? When computer tries to recognize individual what do they rely on?
2. What distinguish between the pretenders and the real identity?
3. Determining an induvial involves 2 steps what are does? Also what is the difference among those two?
4. Why is remote authentication researched among the recent years? Also, over the years computing power have increased, how does this affect in the security industry?
5. There are 4 means of authentication, what are those?
6. What is the difference between multi server authentication and single server authentication?
7. In formal analysis what two kind of methods exist? Also what is formal analysis?
8. In AVISPA what metrics are used?
9. Name the two methods that we learned regarding ‘something user knows’.
10. There are four different type of attacks towards password, what are they? (name and describe them)
11. What is the difference between popular password attack and single account password attack?
12. In BAN logic there are three steps of verification name and describe them in order.
13. Name 4 more attacks on password (Different from the above ones.)
14. How do we store a password? Also in a nut shell, explain the dictionary attack.
15. What is a concealed passwords and what are rainbow tables? (Describe an attack involving the rainbow table.)
16. What are salt values and why do we need them?
17. Describe the Brute Force attack, and what three factors can reduce the amount of time needed to solve a password in brute force attack?
18. In a Linux system, what are the steps to store a password. Also, what does salt values provide?
19. When managing the password file, what is the new/old way? What is the difference among them?
20. What are the four major login authentication scenario?
21. For windows, what are the 2 main method to authenticate a user to local machine?
22. Explain the 3 weakness of the LMHash function.
23. Simply describe how the LMHash function operates.
24. In essence what is bio metric system doing? Describe the three model of biometric system.
25. What is a token and who/what creates them? Also give example of multi layered tokens.
26. What does Federated Identity management schema allow the security system to do? (provide an example)
27. What 2 components does access control affect regarding a computer? Can access control be combination of multiple security service?
28. What is the central element of computer security? What does reference do and what does it mediate?
29. Every OS have three step of authentication process, tell me the steps of that process.
30. What are the three element of access control? Describe them all of them. Also, explain three polices of access control MAC, DAC, RBAC.
31. What is a general approach when performing DAC?
32. What is the subject in context of Access Control Matrix? What types of subject can there be? Why is shared principle bad?
33. What is ACL? What is the difference between ACL and ACM? Also, when is it a good time to use ACL?
34. What is capability list? And when using capability list, what is easy to determine? Also, when a subject have a many tickets – why can this be a problem?
35. How does MAC operate, what is the main difference between DAC an MAC?
36. What is BLP, what kind of attack can it prevent? Also, name the 2 property of BLP.
37. Which property protect information leakage by Trojan horse?
38. What is RBAC and why do we need RBAC?
39. What 2 things does role define and how many mapping can there be between user – role, role – object?
40. How does RBAC makes security management easier?
41. Name 2 advantage of the RBAC?

# Lecture 2 – soltions

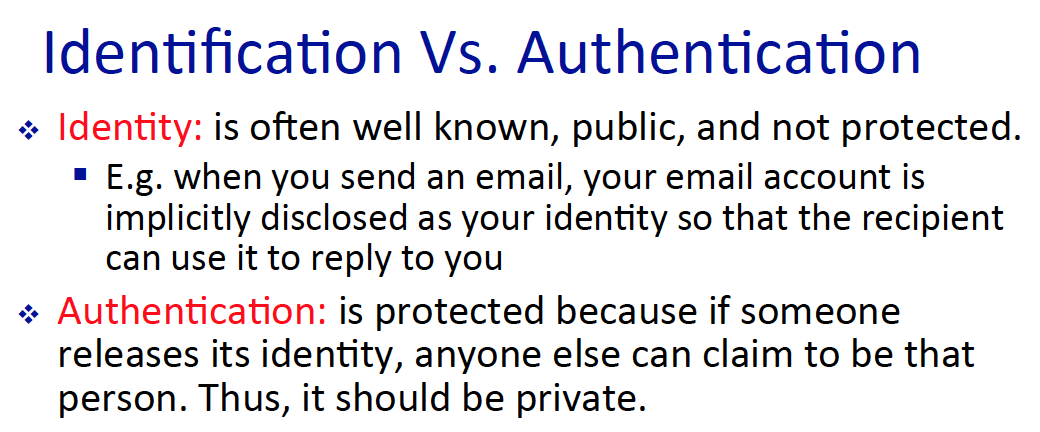
1. What are the tools for security professionals? When computer tries to recognize individual what do they rely on?

* There are three tools for security professionals, which are authentication, access control and cryptography. (Art of cipher text.)

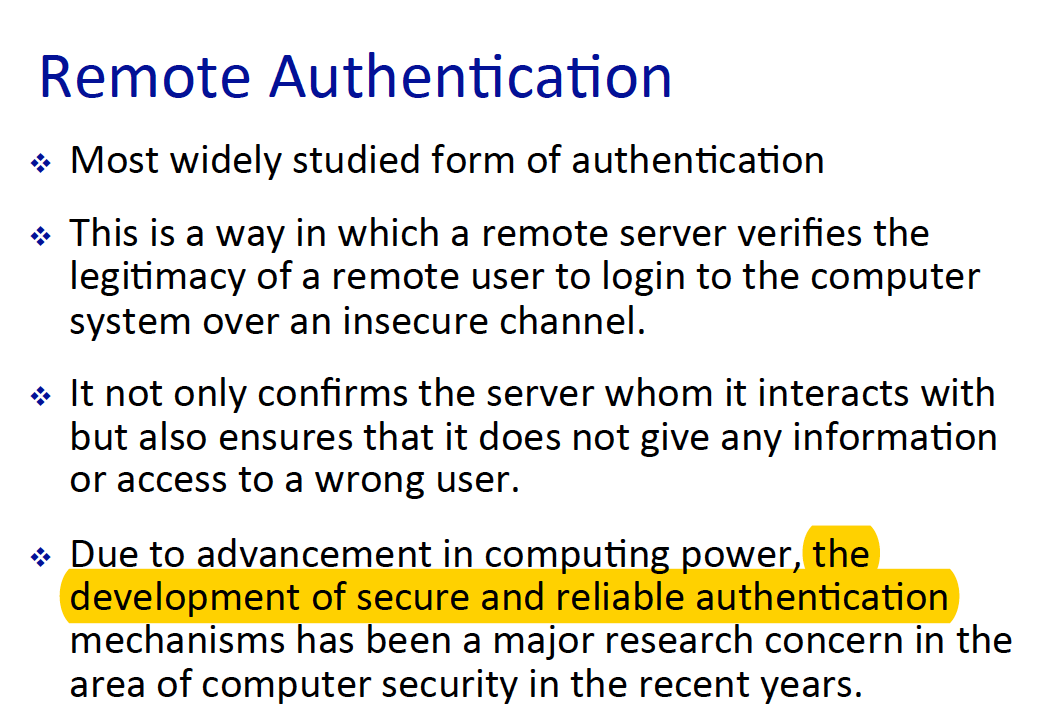
1. What distinguish between the pretenders and the real identity?

* The tool used to distinguish pretender and the real identity is proof by authentication – The authentication itself is a 2 step process the first one is the identification and the second one is the authentication.   
  Identification is when the user provides an identity, telling the system who they are. And authentication is the system, actually verifying the user’s identity. 

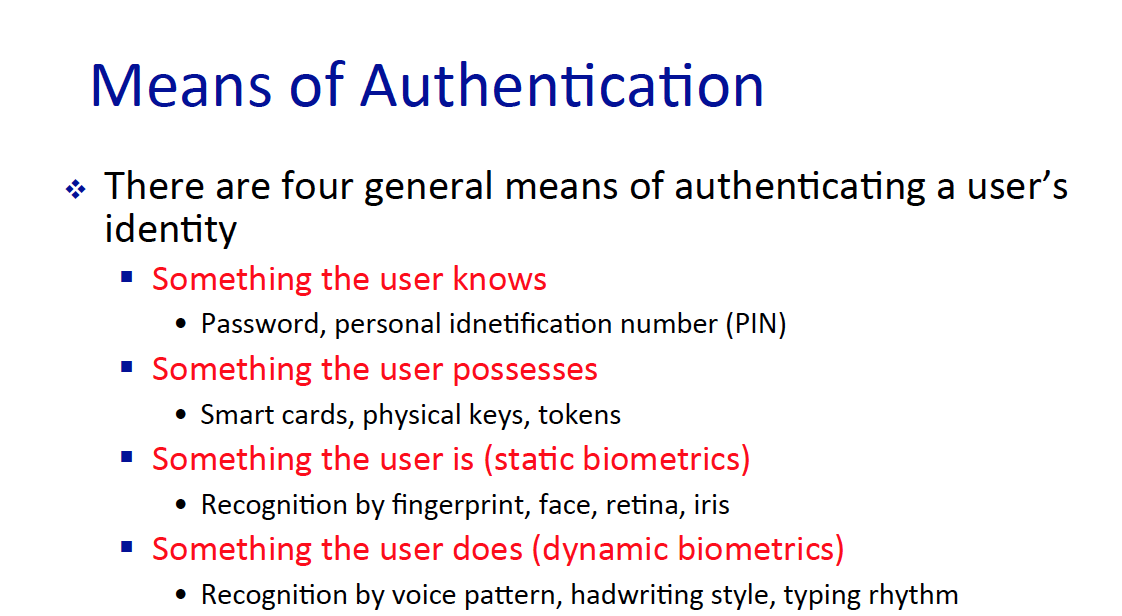
1. Determining an induvial involves 2 steps what are does? Also what is the difference among those two?

* The 2 process is explained above and the difference between those two are, identity can be public, you are who say you are. Anyone can claim to be someone on the web. However, your authentication is not public rather a private information. Since it is verifying your identity. It cannot be a public information.

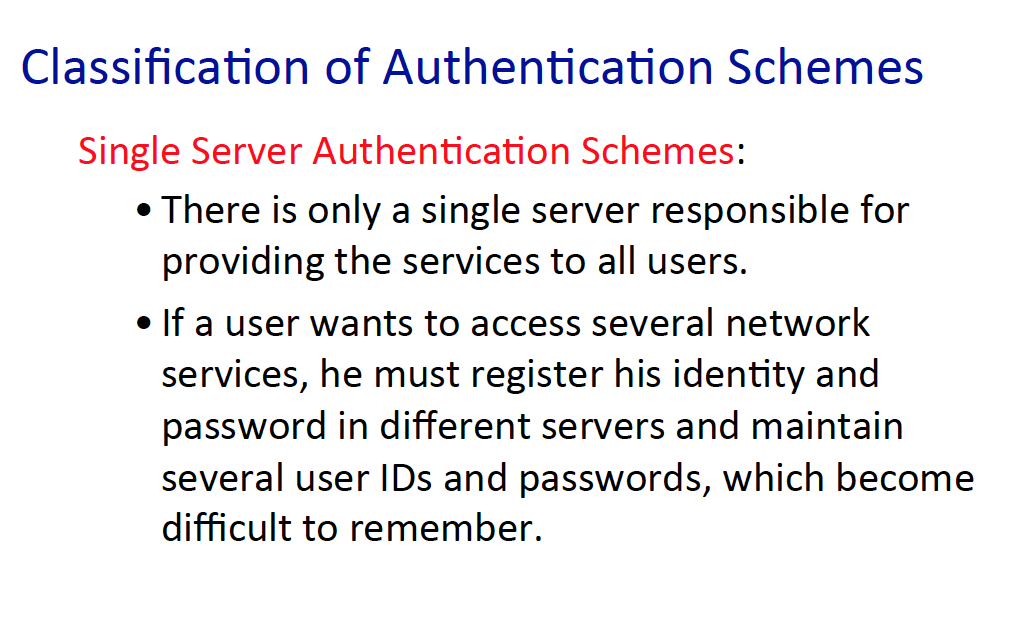
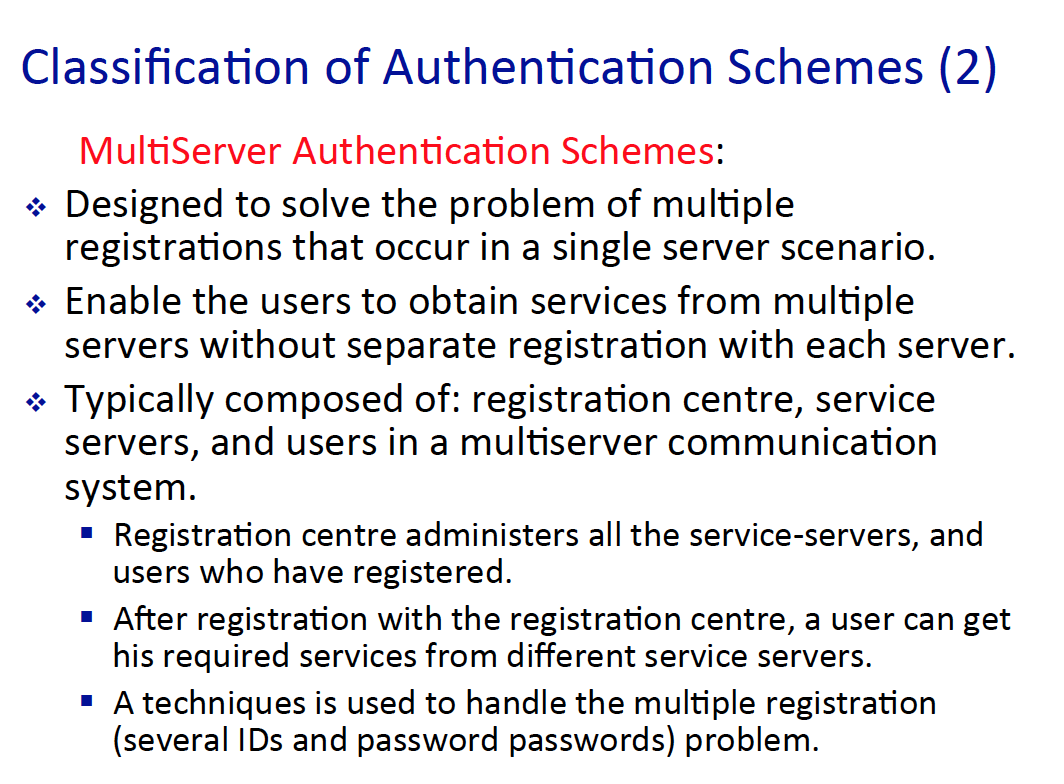
1. Why is remote authentication researched among the recent years? Also, over the years computing power have increased, how does this affect in the security industry?

* The reason for remote authentication is because of the increase of the mobile use, and increase of the devices that are connected to the internet. However, as hardware gets better every year, there is also a negative effect on the computer industry. The encrypted ciphers text are able to be broken in short period amount of time, since the processing power of a computer has increased greatly. 

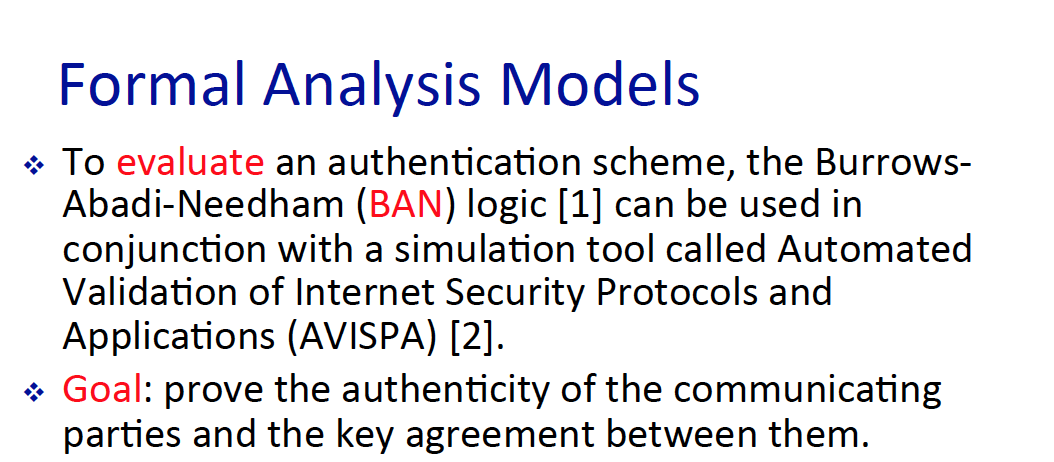
1. There are 4 means of authentication, what are those?

* Something user knows – password, challenge and respond authentication.
* Something user is – static biometric application
* Something user do - dynamic biometric application
* Something user have – security token key, smart card or anything like that.

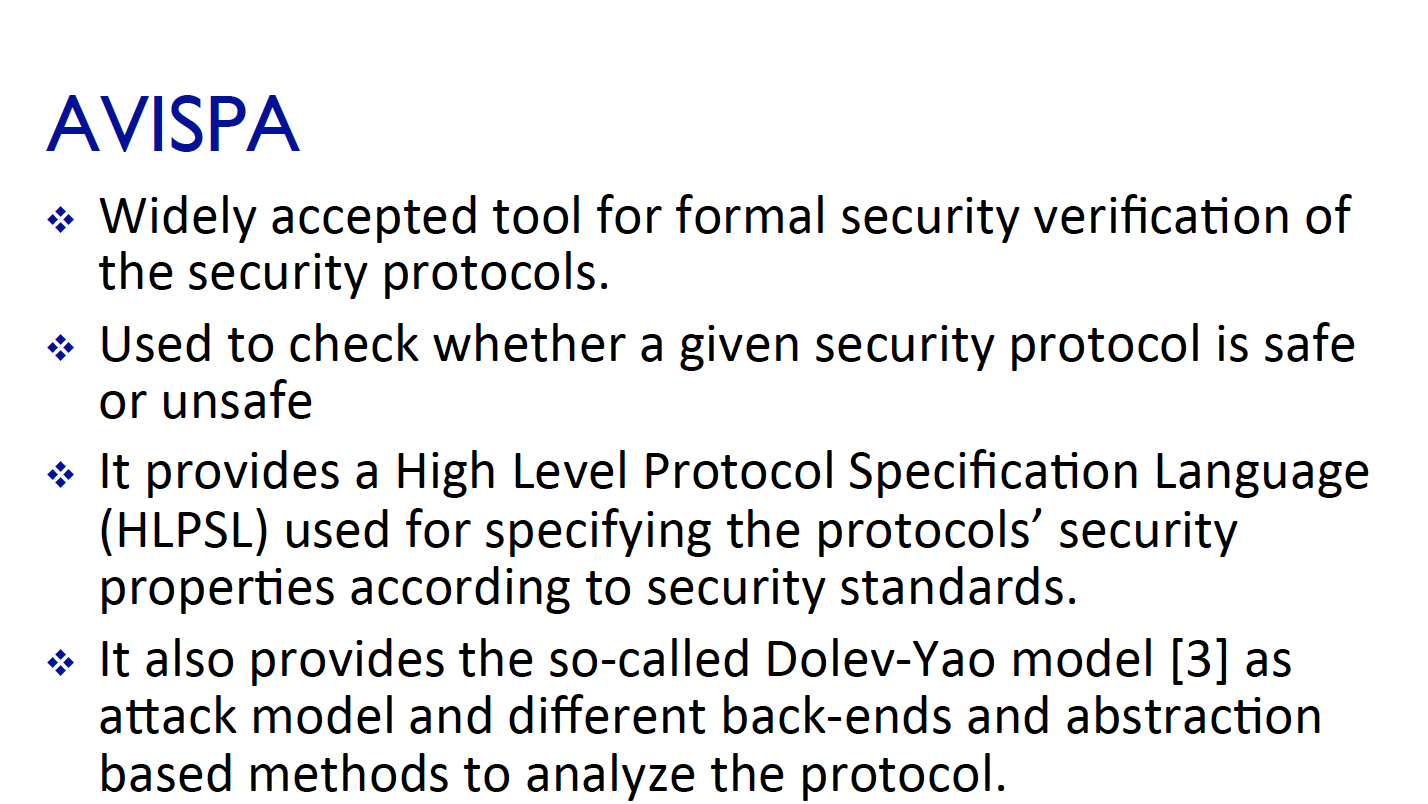
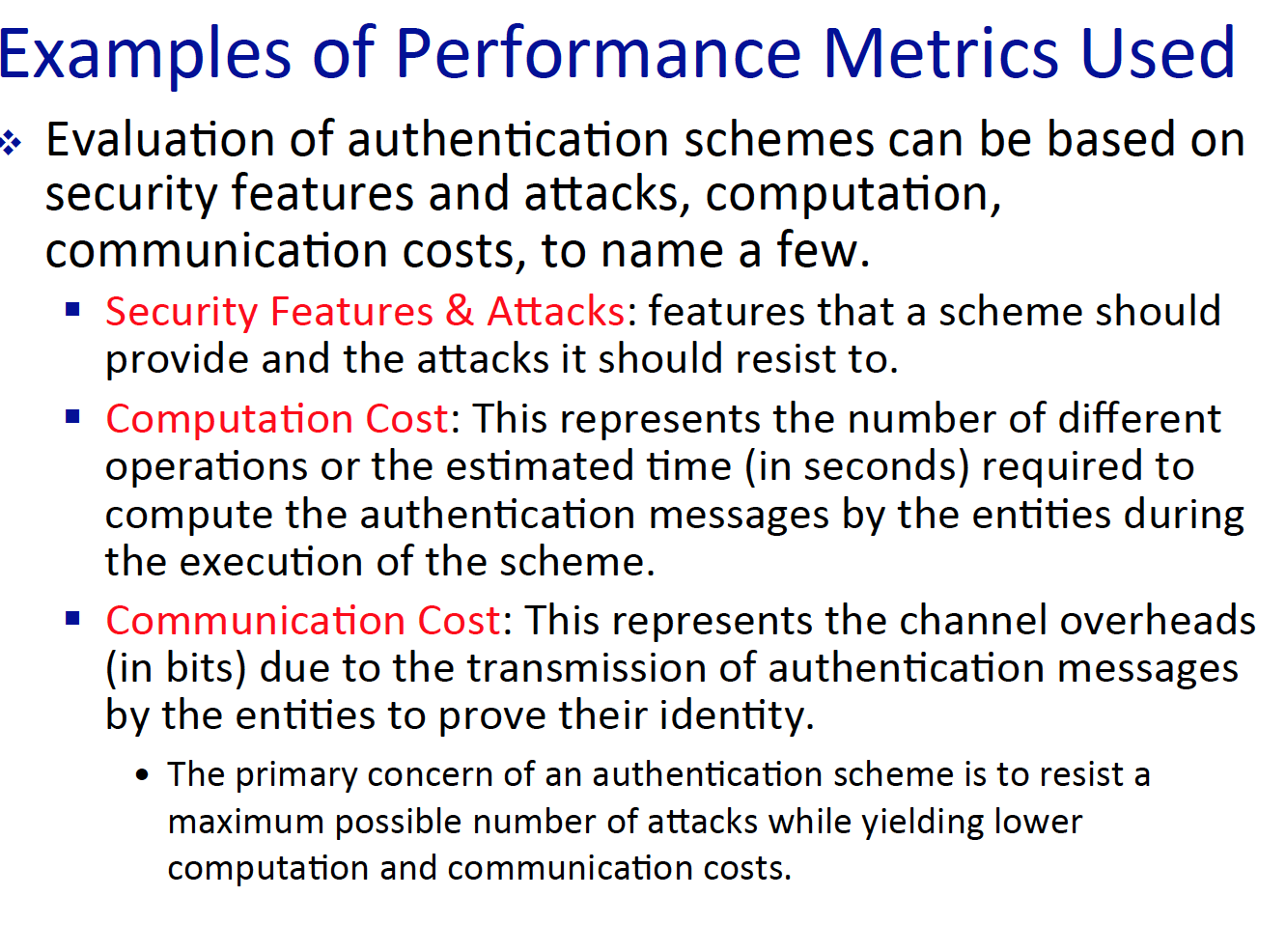
1. What is the difference between multi server authentication and single server authentication?

* The main difference between single server authentication model and multi-server authentication model is that in the single server user have to authenticate multiple times, in order to use each app, they must provide their auth every time. In contrast muti authentication server have an authentication server in which, takes cares of the authentication process. So one authentication is good enough for a user to use multiple apps.

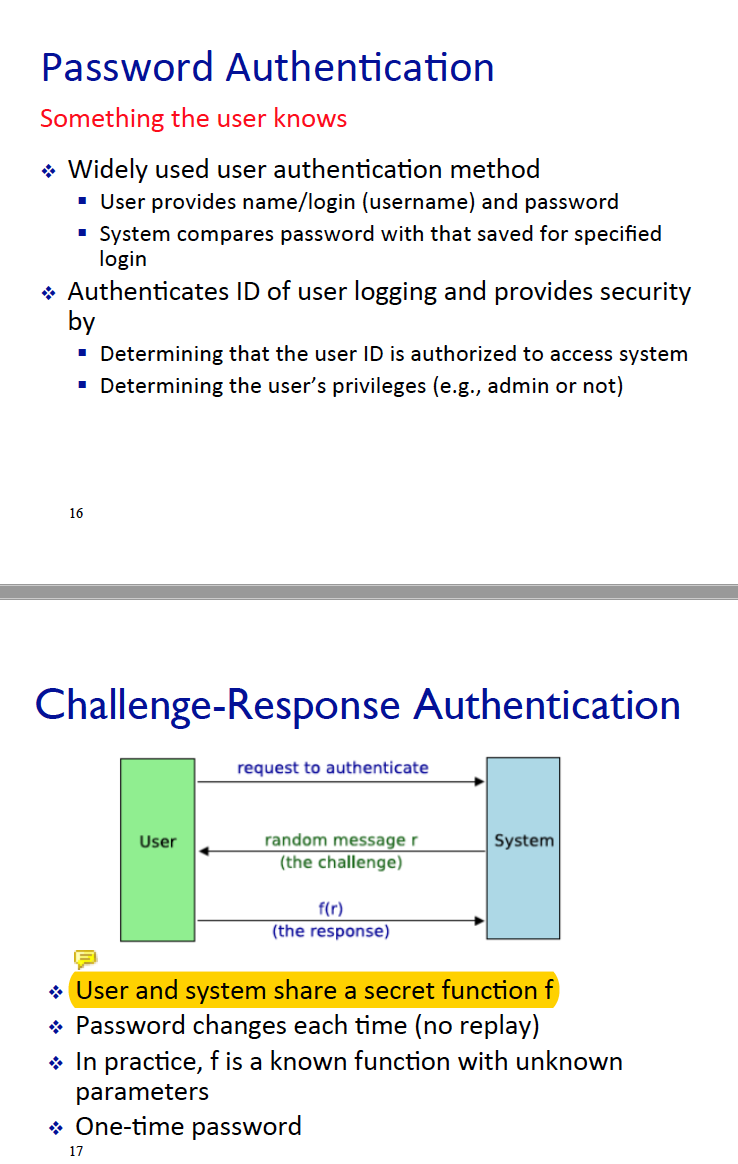
1. In formal analysis what two kind of methods exist? Also what is formal analysis?

* There are BAN logic and Automated Validation of Internet security protocol. And formal analysis is used when two or more host communicate with one another and they need authentication verification.

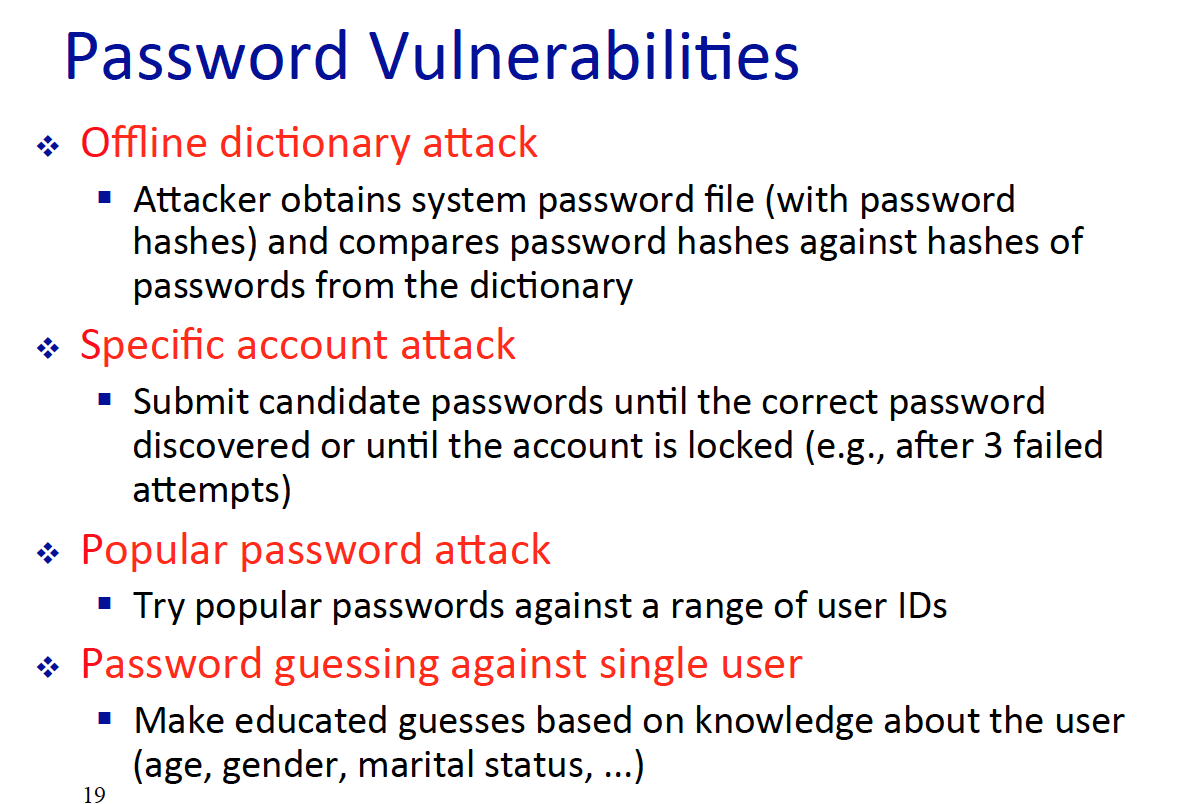
1. In AVISPA what metrics are used?

* In AVISPA, other security protocols are used to measure how safe a particular protocol is. Also, a security protocol standard is used to measure how well security protocol is performing.   
  Also, not only security protocol is measured but also, computational cost and communication cost are measured too.

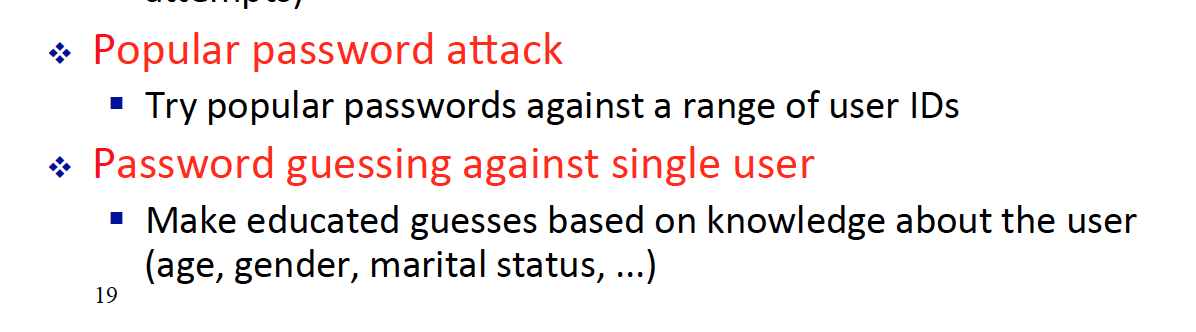
1. Name the two methods that we learned regarding ‘something user knows’.

* We learned the basic password model and one another model is the challenge and respond model. (in which the server challenges the client who want to get authenticated via some text, or process, or even function R).

1. There are four different type of attacks towards password, what are they? (name and describe them)

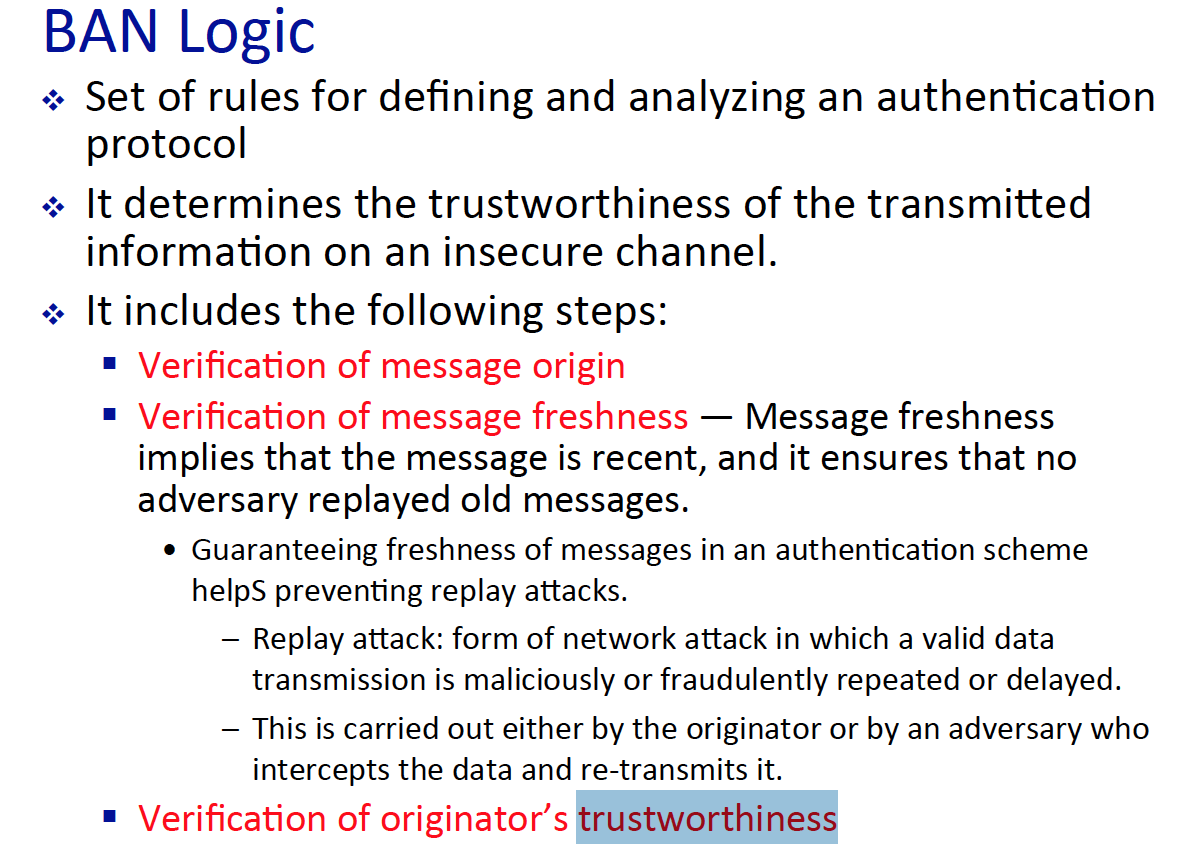
* 1) on/offline dictionary attack – download a dictionary of most used English words and then one by one, perform brute force attack.
* 2) Specific account attack – Submit any type of password, the goal for this attack is to block the user out.
* 3) popular password attack – General attack of using the popular English word attack.
* 4) Educated guess against single user – If the attacker knows something about the user, then they can make an educated guess regarding what is the password.

1. What is the difference between popular password attack and single account password attack?

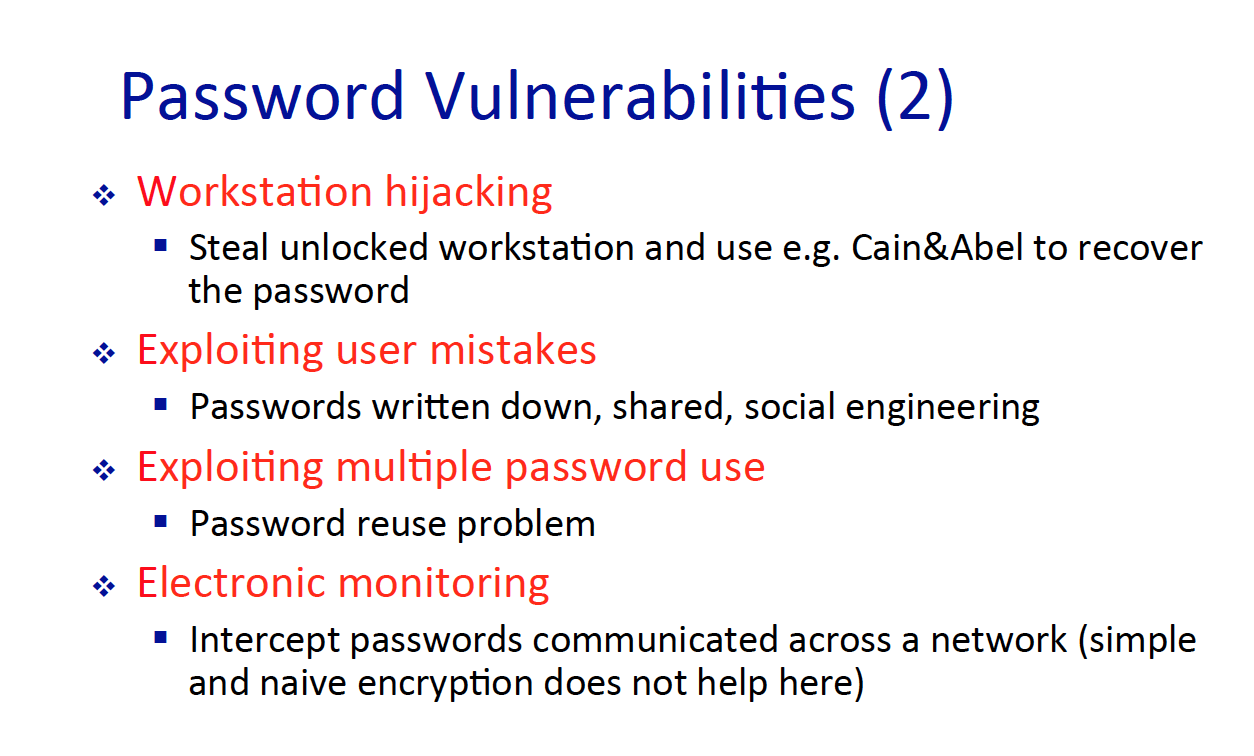
* Popular – general popular used English words, but single account is educated guess on single user.

1. In BAN logic there are three steps of verification name and describe them in order.

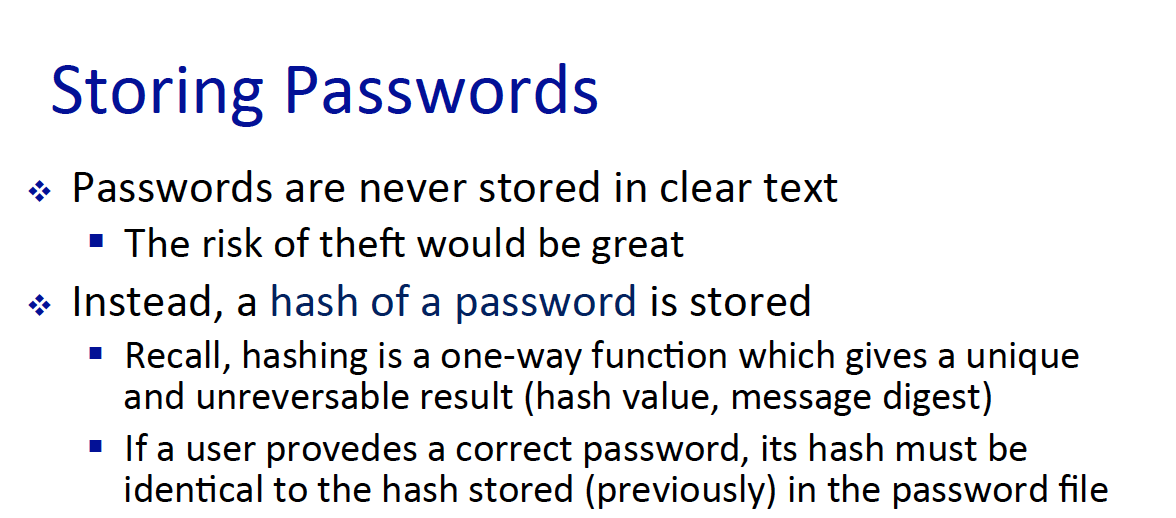
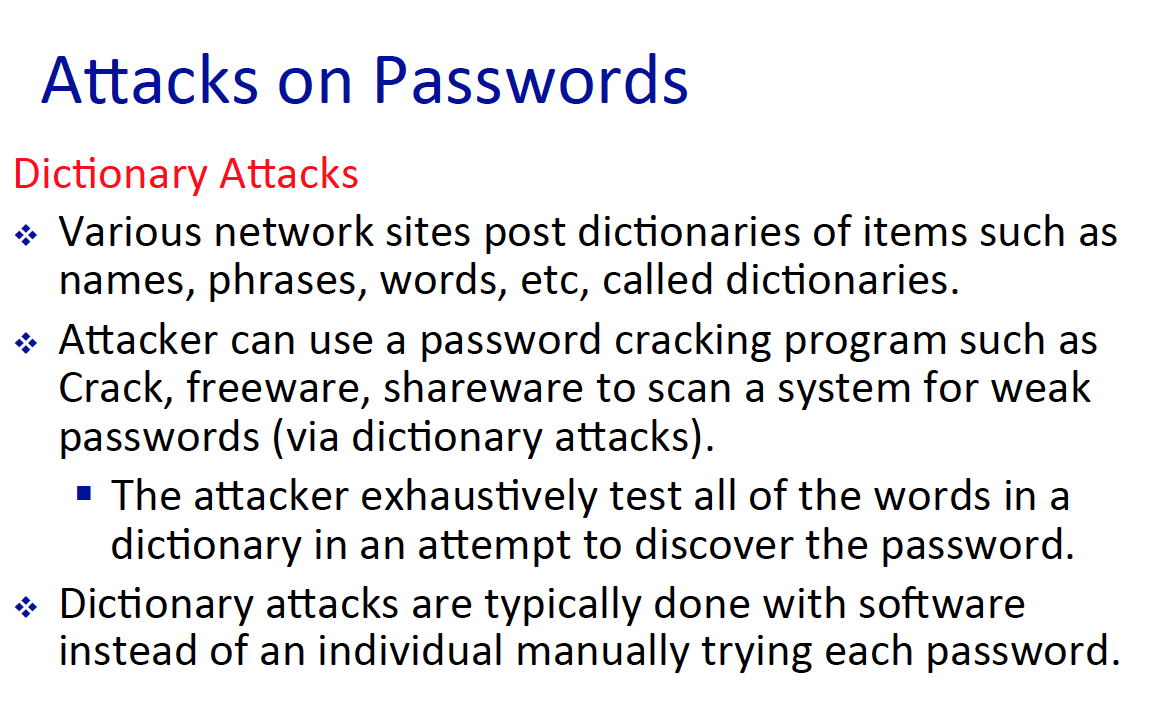
* Verify the message origin – Message authentication, to know exactly show have send the message.
* Verify the message freshness – To verify the message integrity, see whether if the message has been modified or not.
* Verify the originator’s trust trustworthiness – to see if the source of the message is well known or not well known.



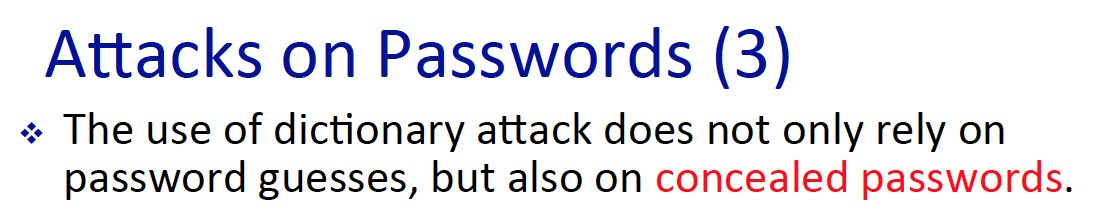
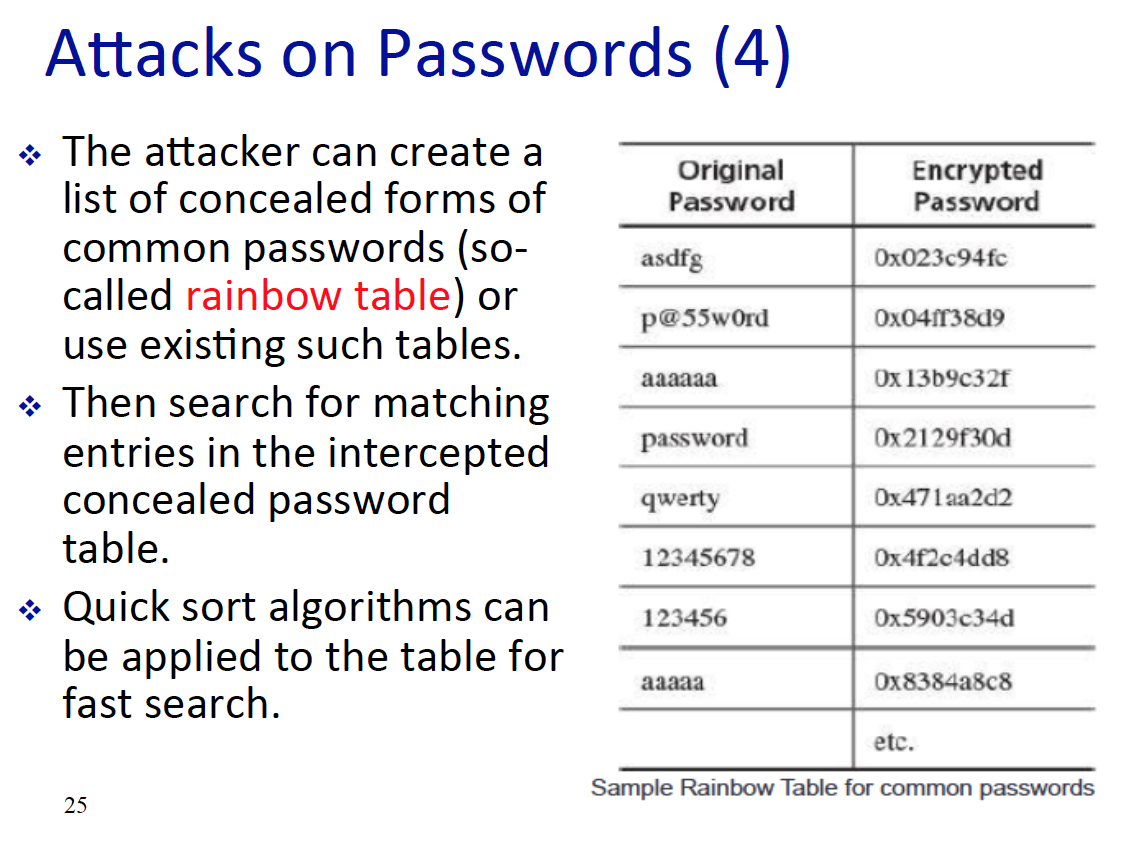
1. Name 4 more attacks on password (Different from the above ones.)

* Stealing the workstation – literality stealing the computer, so this is a violation of physical security.
* Exploiting user mistakes – social engineering, such as written password. And other things.
* Exploiting repeat of password – if the hacker knows one password and the user have been using the password over and over again, then this mistake can be abused.
* Monitoring user activities – Spyware software can record what key have been typed in the password form, - then a cover channel can, deliver that information to the hacker.

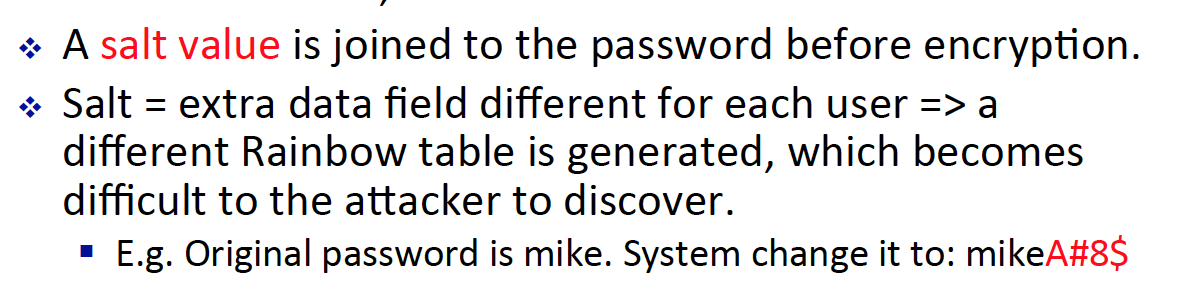
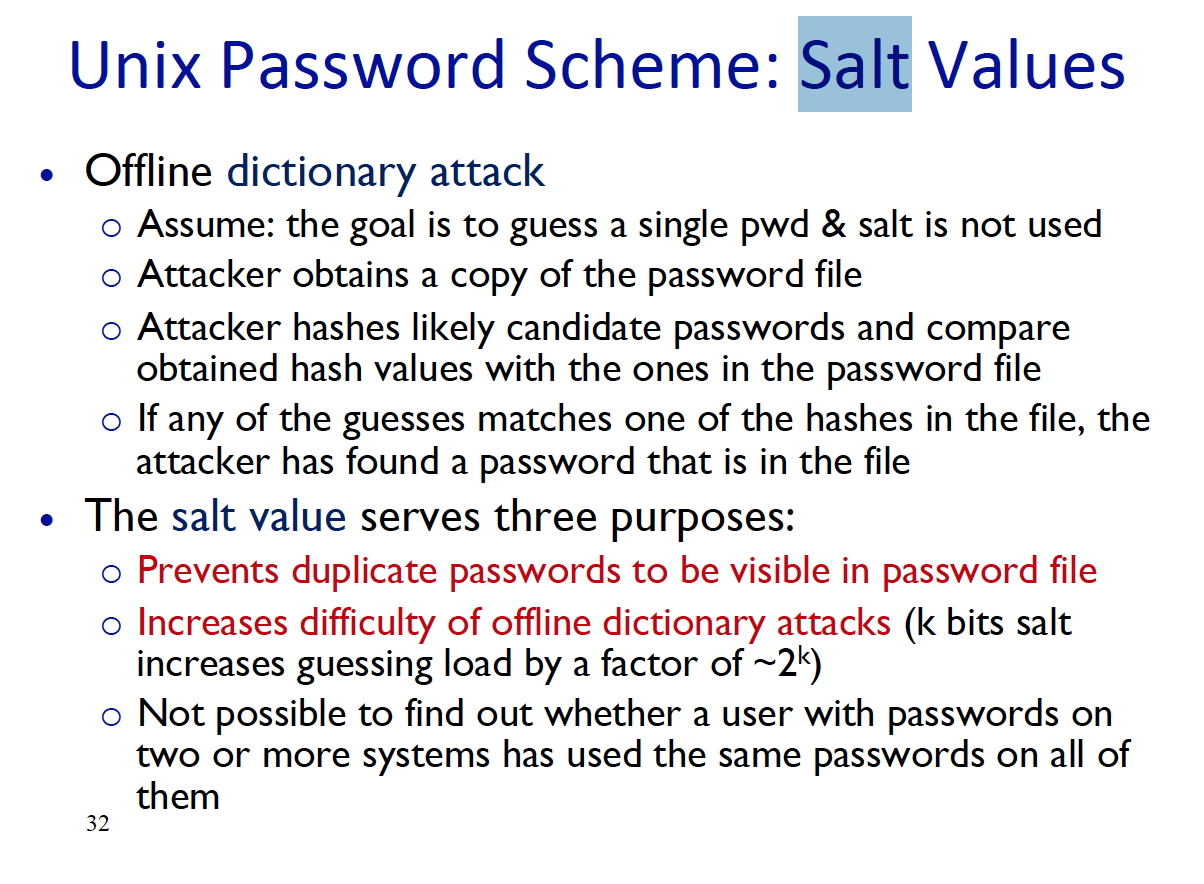
1. How do we store a password? Also in a nut shell, explain the dictionary attack.

* A proper system stores a password as a hash value, hash functions are function in which have a one-way property. It is not easy to recovery what was the original message from the hashed message. But that does not mean that it is 100% secure, tables such as rainbow tables can be used to break the hash function. Rainbow tables are tables that contain both the original message and the hashed message. So the computer can easily compare multiple hashed value by using the table, rather than performing the hash function itself.

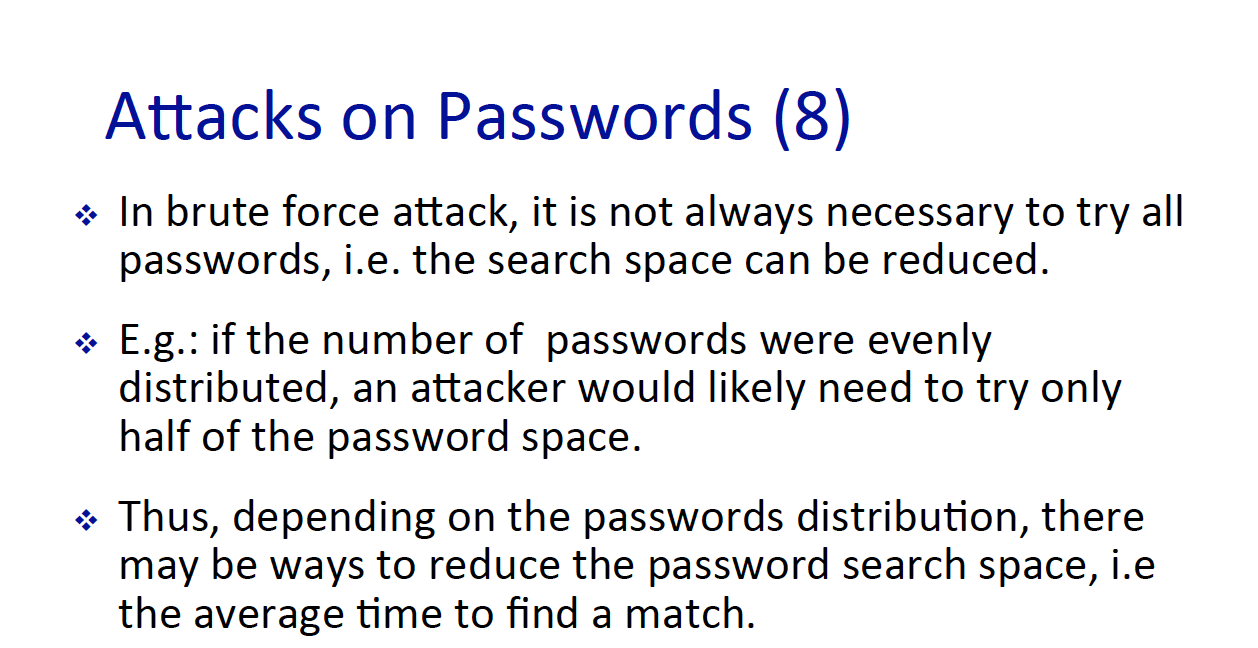
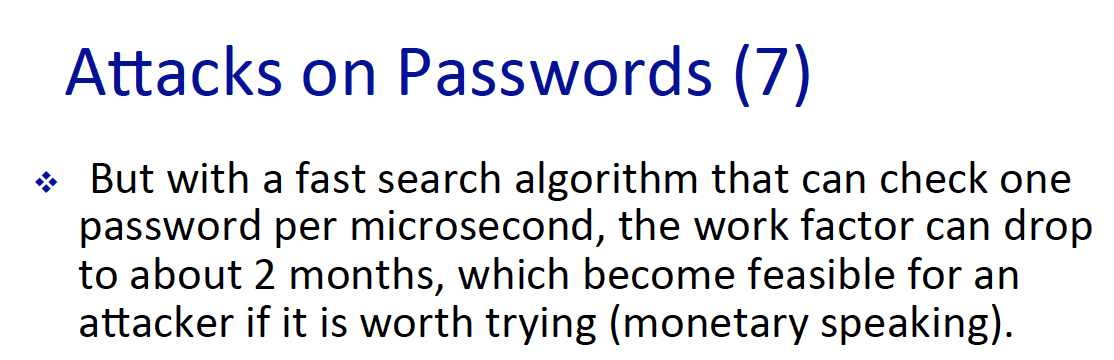
1. What is a concealed passwords and what are rainbow tables? (Describe an attack involving the rainbow table.)

* Rainbow tables are tables that have both original message and encrypted message, usually a hash encryption is used. And concealed password are password that are encrypted. 

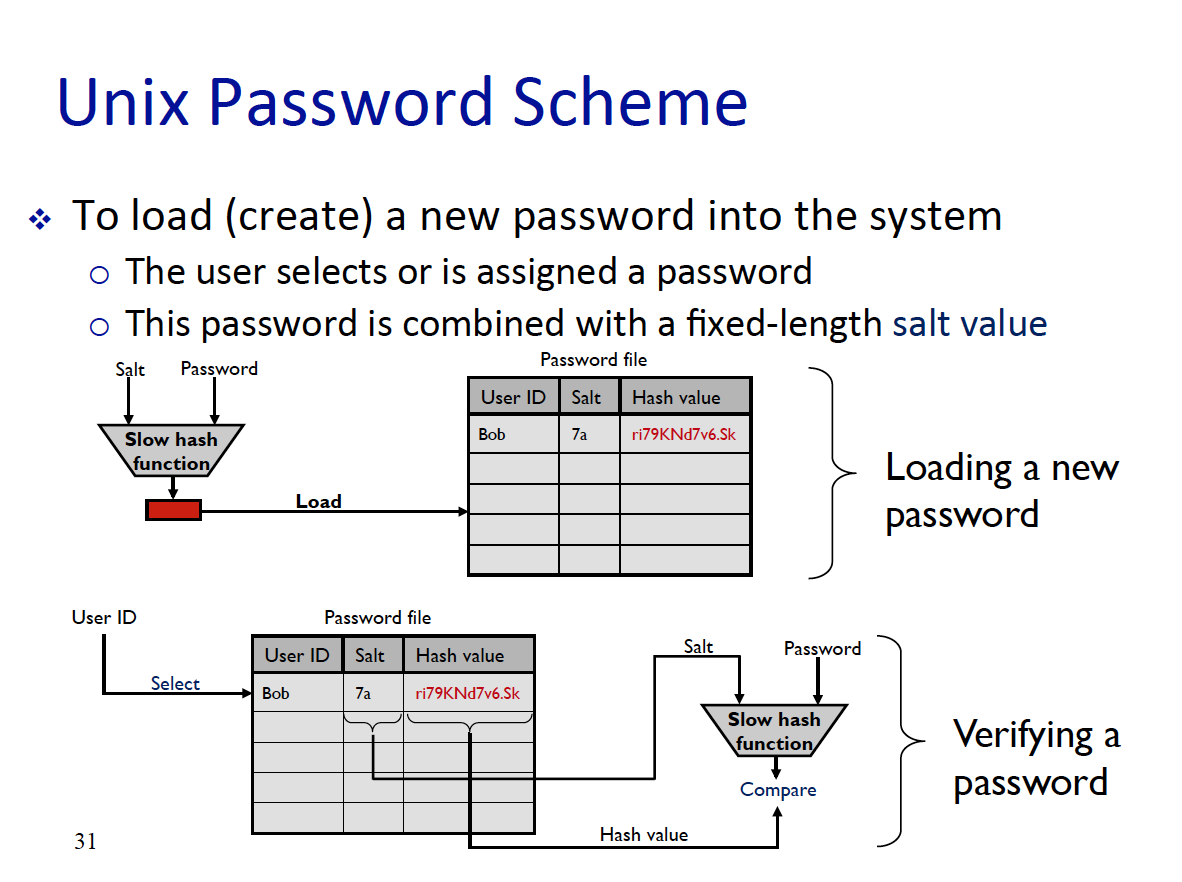
1. What are salt values and why do we need them?

* Salt values are additionally included values to the original text, to make the attack harder since, there are no duplicate password among one another. Also, this have 3 applications   
  1) make password cracking more harder  
  2) The hacker does not know, if the user is using the same password  
  3) Ensure no duplicated passwords

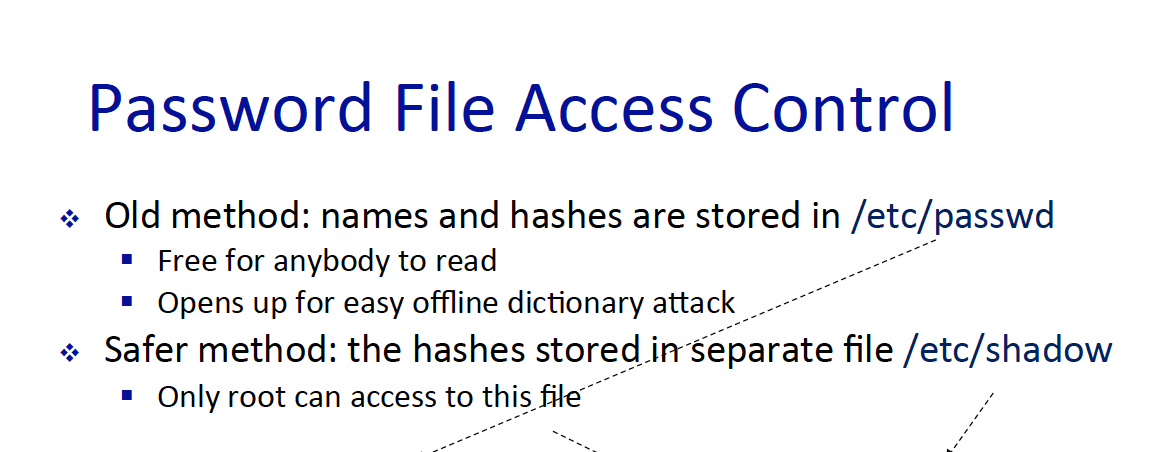
1. Describe the Brute Force attack, and what three factors can reduce the amount of time needed to solve a password in brute force attack?

* Brute force attacks are when the hacker tries every possible value of the password. It is also known as the exhaustion method, since the hacker or the software will get exhausted of guessing a password. The three factors are   
  1) Good hardware – that can handle high complexity task.  
  2) Good algorithm – that have a small O(n) time, to perform the encryption algorithm.  
  3) Statistical attack – calculate the probability of a word being used, then does not have to try all of the possible combination of the English words.

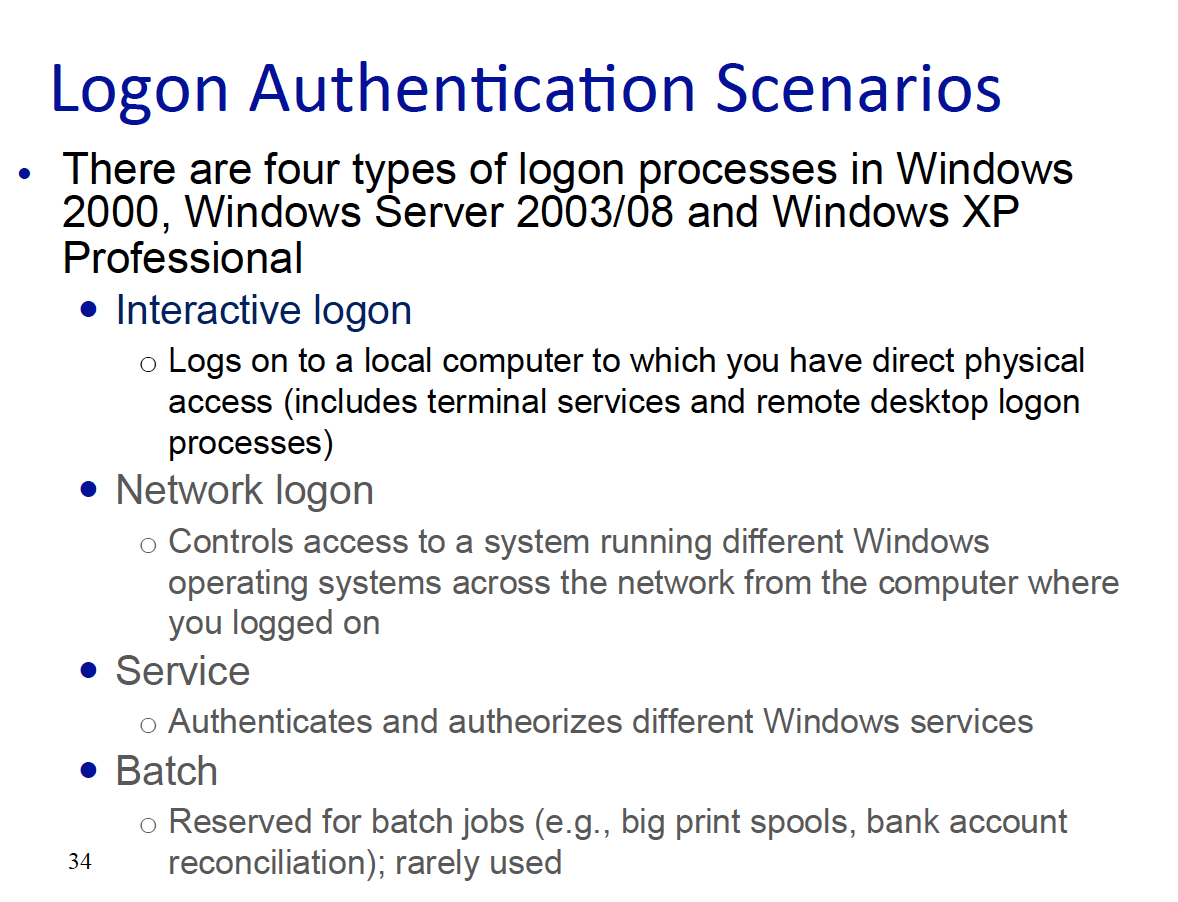
1. In a Linux system, what are the steps to store a password. Also, what does salt values provide?

* The three factor salt value provide is well described above.
* For the Linux system   
  1) The user input a password 2) the os introduce a salt value to add. 3) Then the hashed value is stored in the OS data base.

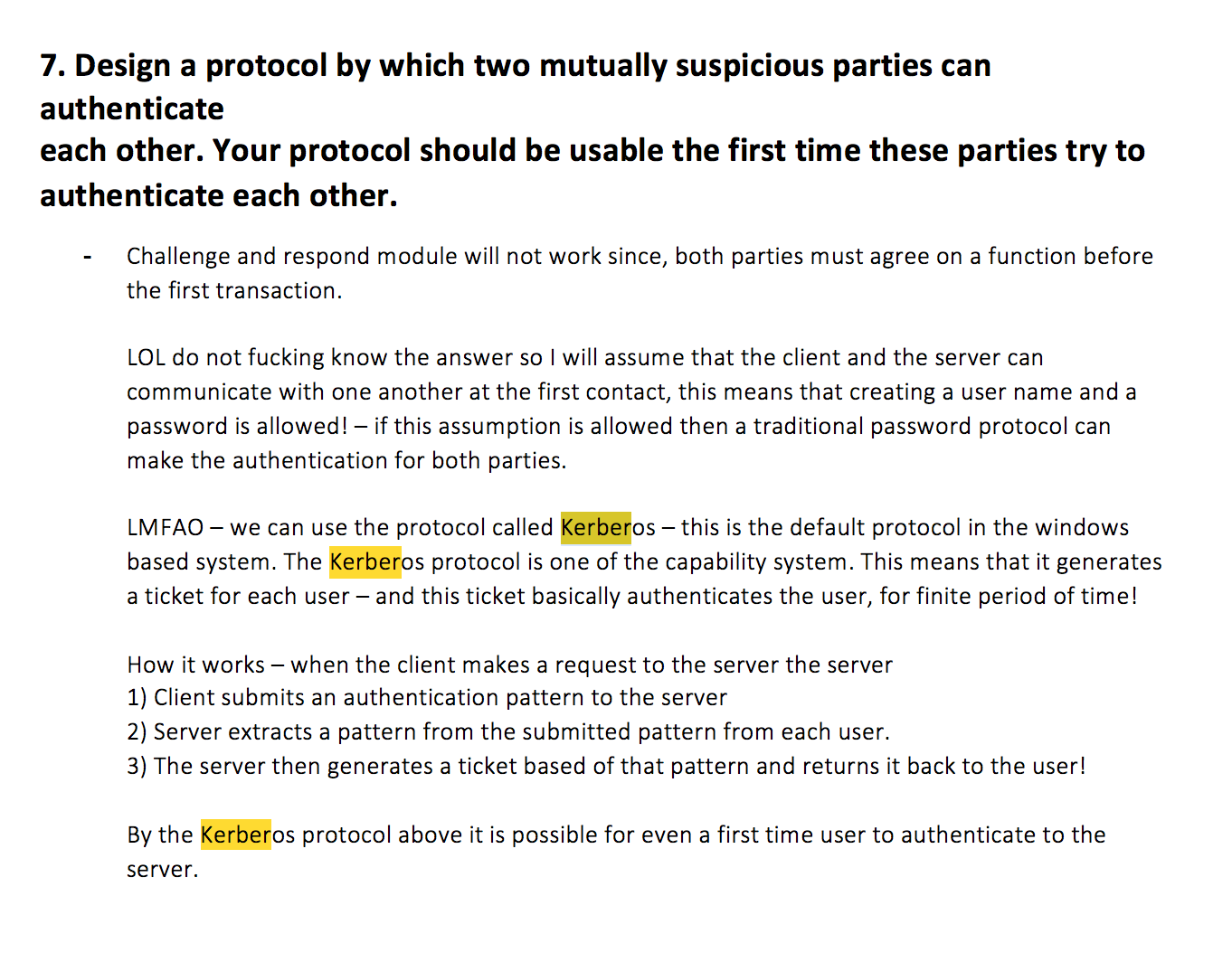
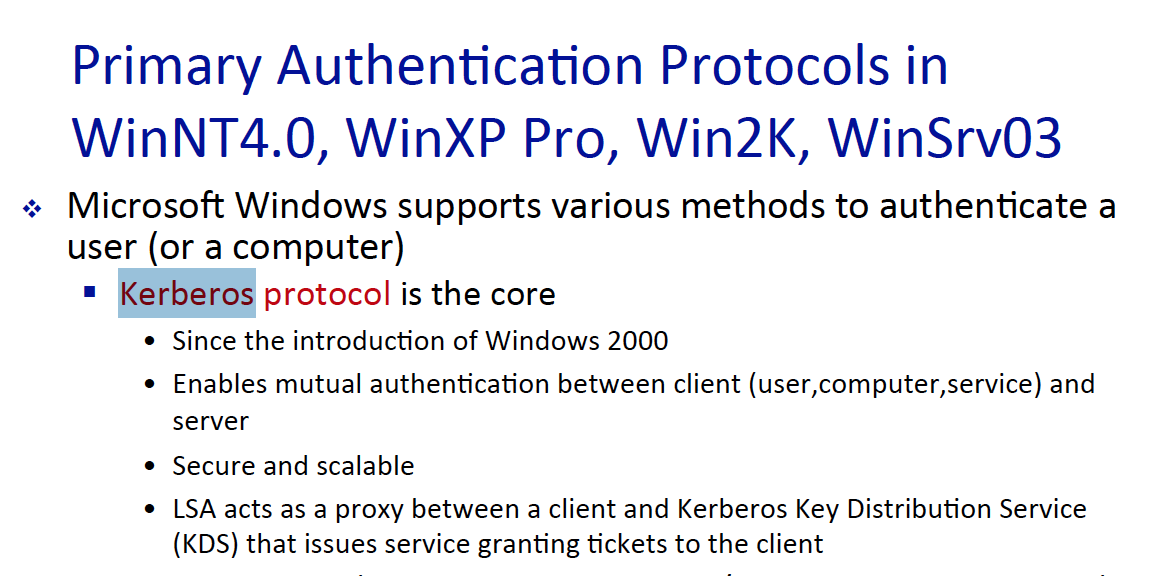
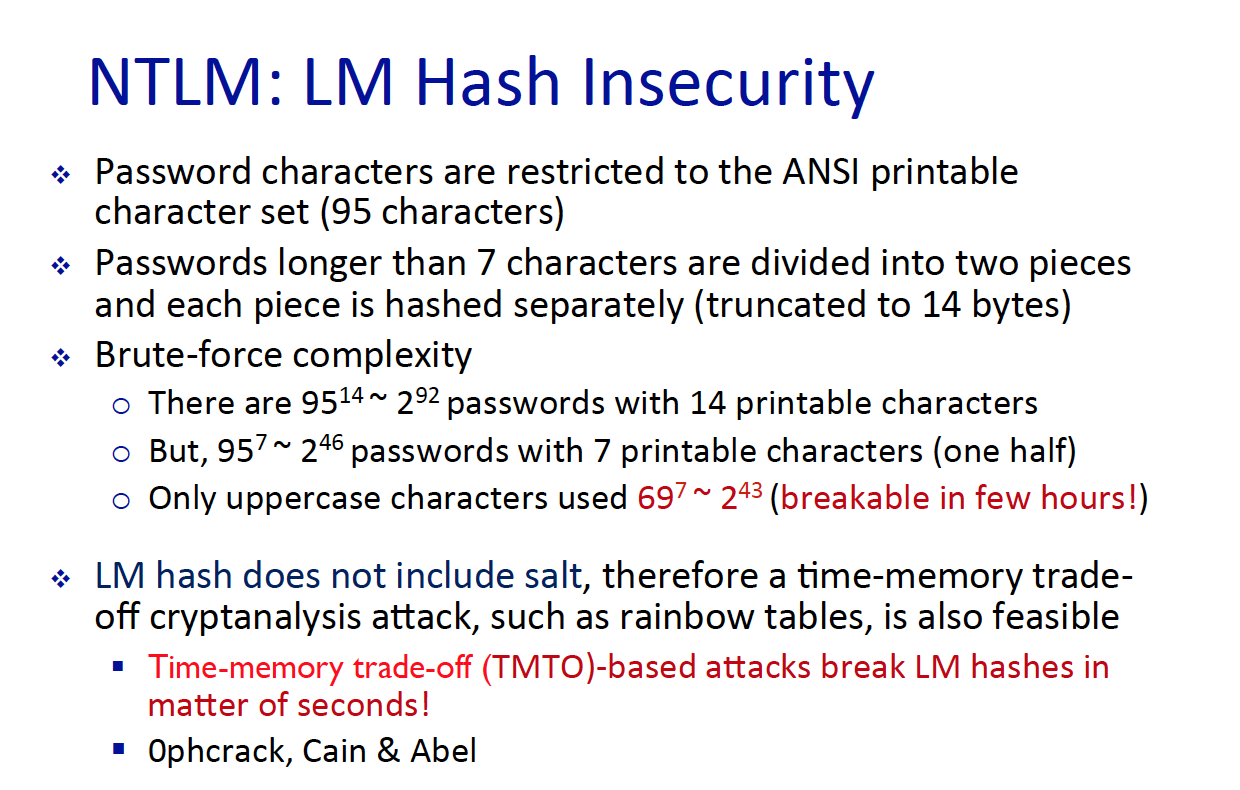
1. When managing the password file, what is the new/old way? What is the difference among them?

* The old way is just to put the rainbow table, anywhere an unauth user can access and the new way is to put it in a folder where it needs a root permission to access the file.

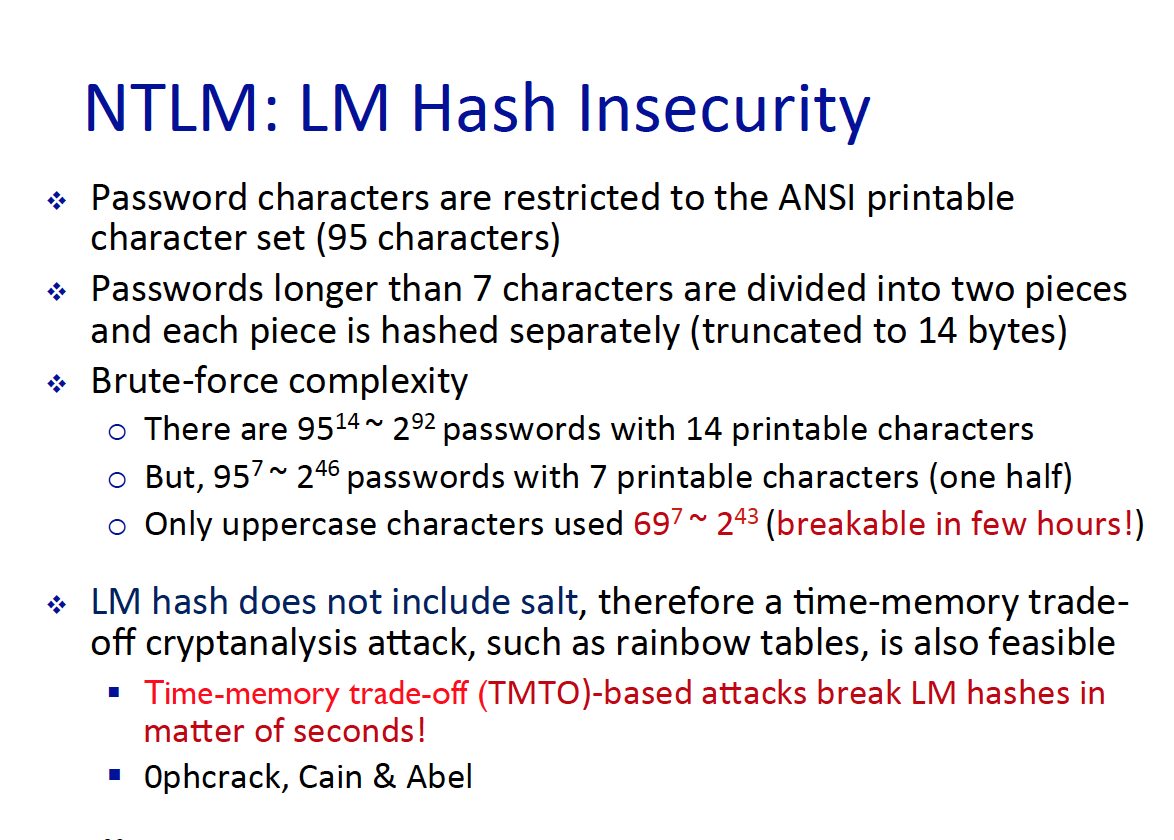
1. What are the four major login authentication scenario?

* For window OS there are 4 major logon models these are .  
  1) Interactive Logon – Access the computer physically, need to be in front of the workstation.   
  2) Network Logon – Remote access, we discussed this. In lecture 5 we talked about web server mediation and in lecture 1 – we talked about the reason how remote access have been researched in the upcoming year.  
  3) Service – To use the window service, either if it is an authenticated service or process that does not need the authentication.   
  4) Batch – rarely used for a batch job. Jae – IDK what is a batch job.

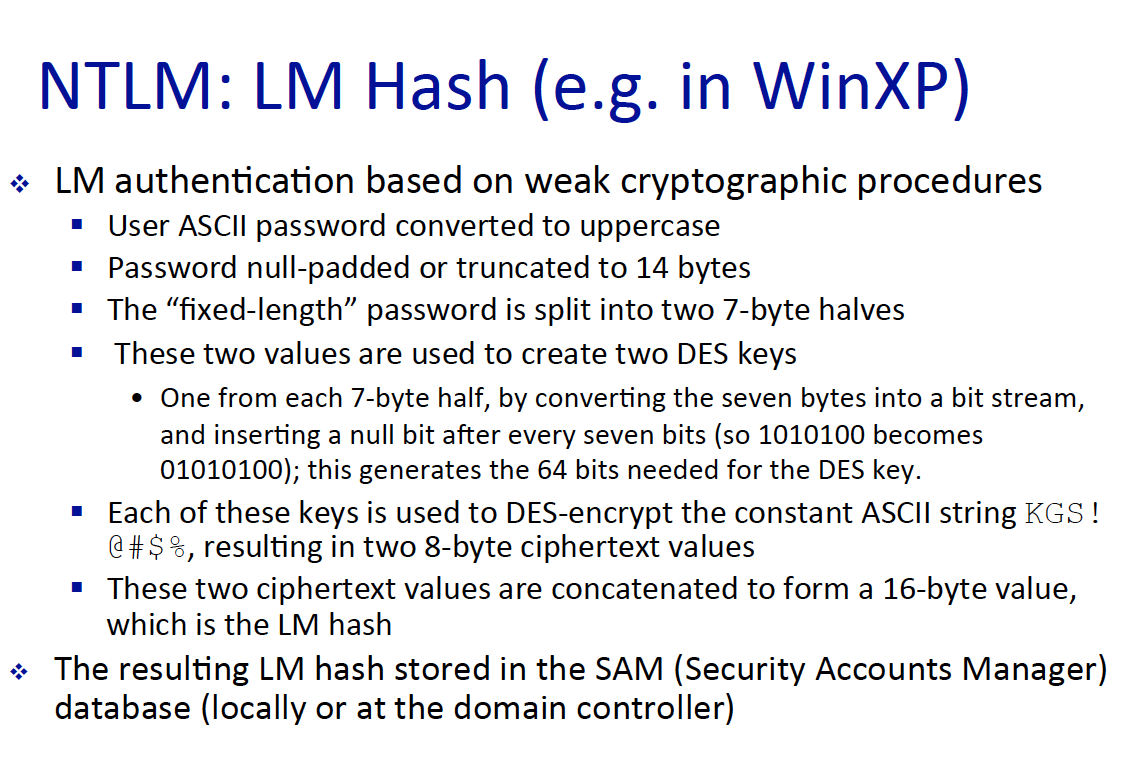
1. For windows, what are the 2 main method to authenticate a user to local machine?

* For windows there are Kerberos and NTLM protocol. kerberos is used when the host want to communicate via remotely and it even can work in the first time two host communicate – Other words does not need a shared key to make the connection possible. – PLEASE LOOK AT MY QUESIOTN SOLVE ON CHAPTER 2 – there are more information regarding what Kerberos is, what can it perform.  
    
  The second one which is NTLM protocol – this is use to authenticate user, using a hash function called, LMHash – this is a weak has function.

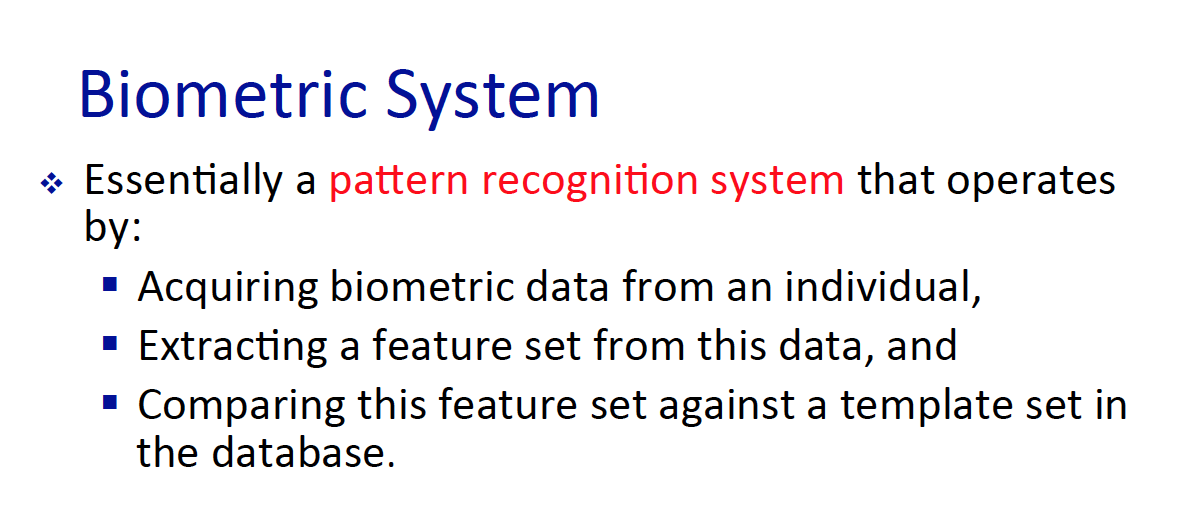
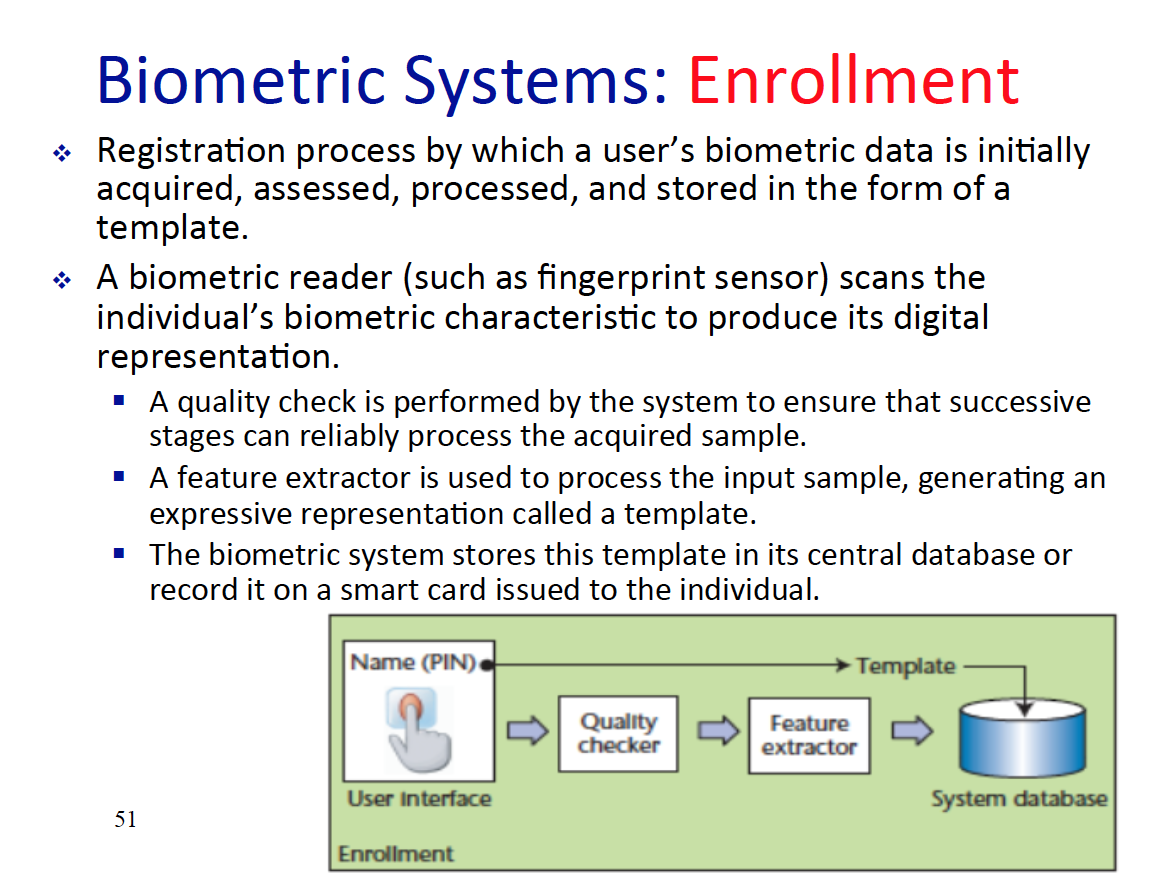
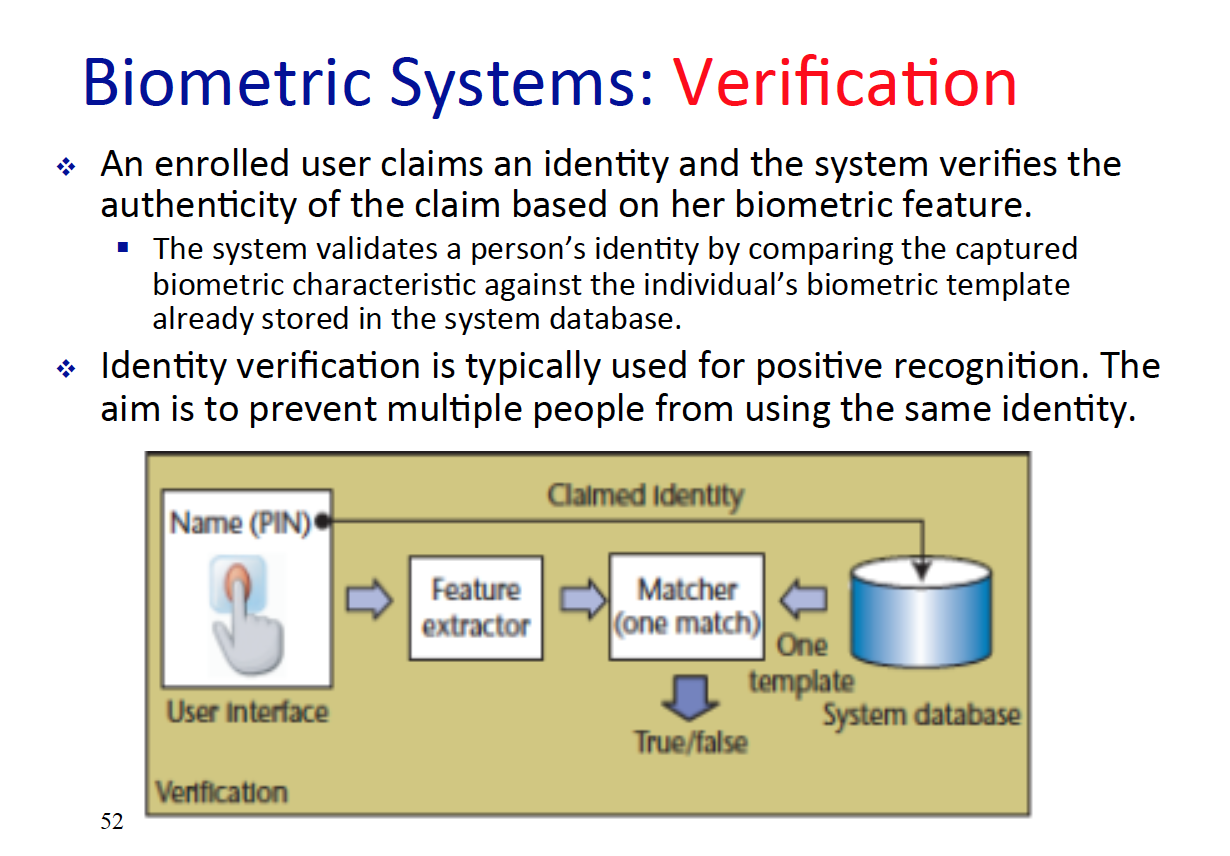
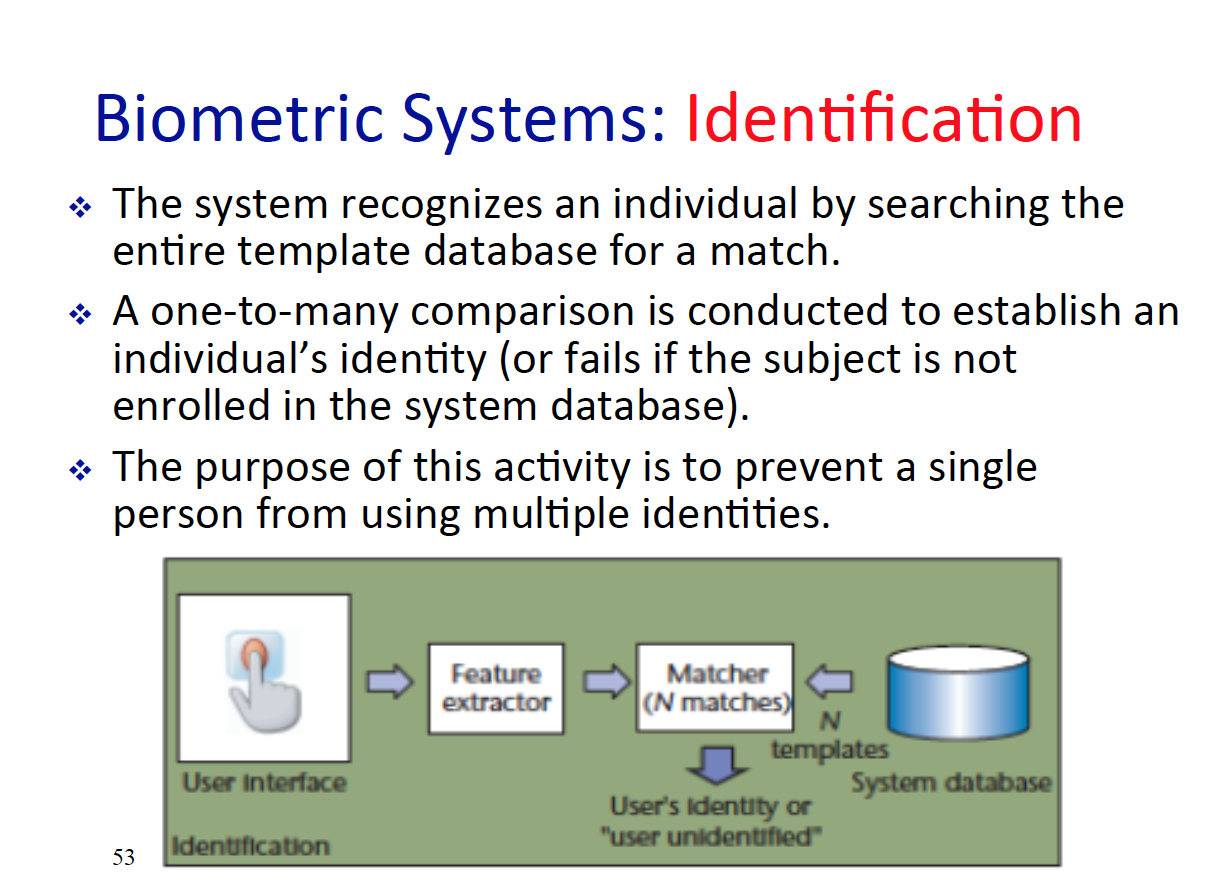
1. Explain the 3 weakness of the LMHash function.

* 1) Only printable ASCII Chars are available as passwords  
  2) All of the inputted chars are converted to Upper case letters  
  3) No salt values are added so, they are valuable to brute force attacks.

1. Simply describe how the LMHash function operates.

* Just read this LOOOOOOL 

1. In essence what is bio metric system doing? Describe the three model of biometric system.

* In essence biometric system is performing pattern recognition. Such as how does an individual finger print look like, extract a feature among the pattern and assign that feature too particular individual.  
  1) enrollment – the first time when the user encounter with the system. This part is the part where the feature extraction happens and then assign to a particular user.   
  2) verification – After the first enrollment the user need to perform authentication – so it gives the system their personal info.  
  3) authentication – Then the system, compares the inputted value with the value that is already in the database. (if match then access is granted)

1. What is a token and who/what creates them? Also give example of multi layered tokens.

* Tokens are something user possess, and this are generally created via the system itself. Multi layered tokens – debit card. The card itself are the token but also the password can be tokens.

1. What does Federated Identity management schema allow the security system to do? (provide an example)
2. What 2 components does access control affect regarding a computer? Can access control be combination of multiple security service?
3. What is the central element of computer security? What does reference do and what does it mediate?
4. Every OS have three step of authentication process, tell me the steps of that process.
5. What are the three element of access control? Describe them all of them. Also, explain three polices of access control MAC, DAC, RBAC.
6. What is a general approach when performing DAC?
7. What is the subject in context of Access Control Matrix? What types of subject can there be? Why is shared principle bad?
8. What is ACL? What is the difference between ACL and ACM? Also, when is it a good time to use ACL?
9. What is capability list? And when using capability list, what is easy to determine? Also, when a subject have a many tickets – why can this be a problem?
10. How does MAC operate, what is the main difference between DAC an MAC?
11. What is BLP, what kind of attack can it prevent? Also, name the 2 property of BLP.
12. Which property protect information leakage by Trojan horse?
13. What is RBAC and why do we need RBAC?
14. What 2 things does role define and how many mapping can there be between user – role, role – object?
15. How does RBAC makes security management easier?
16. Name 2 advantage of the RBAC?