CHAPTER 5

AUTHENTICATION

CHAPTER OUTLINE

After studying this chapter, the students will be able

- Authentication System
- Password Based Authentication, Dictionary Attacks
- Challenge Response System
- Biometric System
- Needham-Schroeder Scheme, Kerberos Protocol

AUTHENTICATION SYSTEM

Authentication is the process of validating the identity of someone or something. It uses information provided to the authenticator to determine whether someone or something is in fact who or what it is declared to be. In private and public computing systems, for example, in computer networks, the process of authentication commonly involves someone, usually the user, using a password provided by the system administrator to **logon**. The user's possession of a password is meant to guarantee that the user is authentic. It means that at some previous time, the user requested, from the system administrator, and the administrator assigned and or registered a self-selected password. The user presents this password to the logon to prove that he or she knows something no one else could know.

Generally, authentication requires the presentation of credentials or items of value to really prove the claim of who you are. The items of value or credential are based on several unique factors that show something you know, something you have, or something you are:

1. **Something you know:** This may be something you mentally possess. This could be a password, a secret word known by the user and the authenticator. Although this is inexpensive administratively, it is prone to people's memory lapses and other weaknesses including secure storage of the password files by the system administrators. The user may use the same password on all system logons or may change it periodically, which is recommended. Examples using this factor include passwords, passphrases, and personal identification numbers (PINs).
2. **Something you have:** This may be any form of issued or acquired self identification such as **SecurID, CryptoCard, ActivCard, SafeWord** and many other forms of **cards and tags**. This form is slightly safer than something you know because it is hard to abuse individual physical identifications. For example, it is harder to lose a smart card than to remember the card number.
3. **Something you are:** This being a naturally acquired physical characteristic such as voice, fingerprint, iris pattern, and other biometrics. Although biometrics is very easy to use, this ease of use can be offset by the expenses of purchasing biometric readers. Examples of items used in this factor include fingerprints, retinal patterns, DNA patterns, and hand geometry.

In addition to the top three factors, another factor, though indirect, also plays a part in authentication.

4. **Somewhere you are:** This usually is based on either physical or logical location of the user. The use, for example, may be on a terminal that can be used to access certain resources.

In general, authentication takes one of the following three forms:

- **Basic authentication** involving a server. The server maintains a user file of either password and user names or some other useful piece of authenticating information. This information is always examined before authorization is granted. This is the most common way computer network systems authenticate users. It has several weaknesses though, including forgetting and misplacing authenticating information such as passwords.

- **Challenge-response**, in which the server or any other authenticating system generates a challenge to the host requesting for authentication and expects a response.
- **Centralized authentication**, in which a central server authenticates users on the network and in addition also authorizes and audits them.

These three processes are done based on server action. If the authentication process is successful, the client seeking authentication is then authorized to use the requested system resources. However, if the authentication process fails, the authorization is denied. The process of auditing is done by the server to record all information from these activities and store it for future use.

MULTIPLE FACTORS AUTHENTICATION

Traditional password-and-username authentication can leave users vulnerable. In 2010 Christopher Chaney, a celebrity obsessed cyber-stalker, got hold of a number of celebrity emails. Using data gleaned from social media and Wikipedia, he successfully guessed the passwords to over 50 personal email accounts belonging to famous women, including Scarlett Johansson, Mila Kunis, and Christina Aguilera. He had access to these accounts for almost a year, and he was responsible for posting nude photos of Scarlett Johanssen and several non-celebrity women. He has since been sentenced to 10 years in jail.

Almost everyone's email address has been exposed online somewhere (luckily there are ways to find out if this has happened). And traditional password-based authentication is inherently insecure. Given these two facts, it's essential to offer customers additional ways to protect their accounts.

Multi-factor authentication (MFA) is an extra authentication method that's becoming increasingly common. Multifactor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Typical MFA scenarios include:

- Swiping a card and entering a PIN.
- Logging into a website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the requester's phone or email address.
- Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to a network.
- Swiping a card, scanning a fingerprint and answering a security question.
- Attaching a USB hardware token to a desktop that generates a one-time passcode and using the one-time passcode to log into a VPN client.

TYPES OF AUTHENTICATION

Earlier, we identified three factors that are used in the positive authentication of a user. We also pointed out in the previous section that while these factors are in themselves good, there are items in some that suffer from vulnerabilities. Table 5.1 illustrates the shortcomings of user identity characteristics from the factors that suffer from these vulnerabilities.

Table 5.1: Authentication factors and their vulnerabilities

Number	Factor	Examples	Vulnerabilities
1	What you know?	Password, PIN	Can be forgotten, guessed, duplicated
2	What you have?	Token, ID Card, Keys	Can be lost, stolen, duplicated
3	What you know?	Iris, voiceprint, fingerprint	Nonrepudiable

From table 5.1, one can put the factors into two categories: nonrepudiable and repudiable authentication. Other types of authentication include user, client, and session authentication.

a) **Nonrepudiable Authentication**

Nonrepudiable authentication involves all items in factor 3. Recall that factor three consists of items that involve some type of characteristics and whose proof of origin cannot be denied. The biometrics used in factor 3, which include iris patterns, retinal images, and hand geometry, have these characteristics. Biometrics can positively verify the identity of the individual. The biometric characteristics cannot be forgotten, lost, stolen, guessed, or modified by an intruder. They, therefore, present a very reliable form of access control and authorization. It is also important to note that contemporary applications of biometric authorization are automated, which further eliminates human errors in verification. As technology improves and our understanding of the human anatomy increases, newer and more sensitive and accurate biometrics will be developed.

b) **Repudiable Authentication**

The first two factors, "what you know" and "what you have," are factors that can present problems to the authenticator because the information presented can be unreliable. It can be unreliable because such factors suffer from several well-known problems including the fact that possessions can be lost, forged, or easily duplicated. Also knowledge can be forgotten and taken together, knowledge and possessions can be shared or stolen. Repudiation is, therefore, easy. Before the development of items in factor 3, in particular the biometrics, authorization, and authentication methods relied only on possessions and knowledge.

AUTHENTICATION METHODS

Different authentication methods are used based on different authentication algorithms. These authentication methods can be combined or used separately, depending on the level of functionality and security needed. Among such methods are

- Password authentication,
- Public-key authentication,
- Anonymous authentication,
- Remote authentication and
- Certificate-based authentication.

PASSWORD BASED AUTHENTICATION, DICTIONARY ATTACKS

The password authentication methods are the oldest and the easiest to implement. They are usually set up by default in many systems. Sometimes, these methods can be interactive using the newer keyboard-interactive authentication.

REUSABLE PASSWORDS

There are two types of authentication in reusable password authentication: user and client authentication.

- **User authentication:** This is the most commonly used type of authentication, and it is probably the most familiar to most users. It is always initiated by the user, who sends a request to the server for authentication and authorization for use of a specified system resource. On receipt of the request, the server prompts the user for a user name and password. On submission of these, the server checks for a match against copies in its database. Based on the match, authorization is granted.
- **Client authentication:** Normally, the user requests for authentication and then authorization by the server to use a system or a specified number of system resources. Authenticating users does not mean the user is free to use any system resource the user wants. Authentication must establish user authorization to use the requested resources in the amount requested and no more. This type of authentication is called client authentication. It establishes users' identities and controlled access to system resources.

Because these types of authentication are the most widely used authentication methods, they are the most abused. They are also very unreliable because users forget them, they write them down, they let others use them, and most importantly, they are easy to guess because users choose simple passwords. They are also susceptible to cracking and snooping. In addition, they fall prey to today's powerful computers, which can crack them with brute force through exhaustive search.

ONE-TIME PASSWORDS

One-time password authentication is also known as session authentication. Unlike reusable passwords that can be used over extended periods of time, one-time passwords are used once and disposed of. They are randomly generated using powerful random number generators. This reduces the chances of their being guessed. In many cases they are encrypted, then issued to reduce their being intercepted if they are sent in the clear. There are several schemes of one-time passwords. The most common of these schemes are S/Key and token.

- **S/Key password** is a one-time password generation scheme defined in RFC 1760 and is based on MD4 and MD5 encryption algorithms. It was designed to fight against replay attacks where, for example, in a login session, an intruder eavesdrops on the network login session and gets the password and user-ID for the

legitimate user. Its protocol is based on a client-server model in which the client initiates the S/Key exchange by sending the first packet to which the server responds with an ACK and a sequence number. The client then responds to the server by generating a one-time password and passes it to the server for verification. The server verifies the password by passing it through a hash function and compares the hash digest to the stored value for a match.

- **Token password** is a password generation scheme that requires the use of a special card such as a smart card. According to Kaeo, the scheme is based on two schemes: challenge-response and time-synchronous. In a time-synchronous scheme, an algorithm executes both in the token and on the server and outputs are compared for a match. These numbers, however, change with time.

Although they are generally safer, one-time passwords have several difficulties including synchronization problems that may be caused by lapsed time between the timestamp in the password and the system time. Once these two times are out of phase, the password cannot be used. Also synchronization problems may arise when the one-time password is issued based on either a system or user. If it is based on the user, the user must be contacted before use to activate the password.

DICTIONARY ATTACK

A method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password. For example, let's say that Bob encrypted his hard drive with the password "hunter2". Alice then uses a dictionary attack to try every possible word in the dictionary. If "hunter2", Bob's password, is in the dictionary – then Alice will have the key and be able to get access to Bob's hard drive.

While using words in the dictionary, as well as any derivatives of those words known as leetspeak (character replacement with alphanumeric and non-alphanumeric characters) is common, the dictionary in these types of attacks can also be a collection of previously leaked passwords or key phrases.

It is estimated that around **80% of people re-use their passwords** across online platforms including social media, personal banking, and even work-related systems. While this may seem like a good way to help remember your passwords for important accounts, it is actually leaving you vulnerable to a data breach. No one understands this more than Facebook CEO, Mark Zuckerberg, who had his social media accounts compromised – including Twitter, where hackers tweeted from his account. The hackers revealed that the famous CEO's password had been compromised in the LinkedIn data breach. His password for his LinkedIn account, dadada, was also used for his Twitter and other compromised social media accounts.

These types of attacks can have huge ramifications for your business. Dropbox suffered a breach in 2012 that stemmed from an employee using the same password for LinkedIn that they used for their corporate Dropbox account. Instead of some careless tweets from a hacker, this breach resulted in the theft of 60 million user credentials.

PREVENTING A DICTIONARY ATTACK

The length of the password is an effective defense against brute-force attacks. The best strategy for creating a long password, that is also memorable, is to make it a passphrase. A passphrase is a sentence or phrase, with or without spaces, typically more than 20 characters longer. The words making up a passphrase should be meaningless together to make them less susceptible to social engineering. But a passphrase is only a good choice when it doesn't appear on a list of leaked passwords.

Blacklisting these leaked passwords is an effective way to protect your organization from falling victim to a password dictionary attack. Cyber security expert Troy Hunt manages one of the largest collections of leaked passwords on his site Have I Been Pwned (https://haveibeenpwned.com/) where you can personally search to see if your credentials have ever been leaked.

Another critical measure to prevent a dictionary attack is to stop password reuse between different password-protected systems. User training can help educate on the importance of not reusing passwords. However, the only way to remove this possibility is to blacklist leaked passwords at password creation.

CHALLENGE RESPONSE SYSTEM

In previous section, we briefly talked about challenge-response authentication as another form of relatively common form of authentication. Challenge-response, as a password authentication process, is a handshake authentication process in which the authenticator issues a challenge to the user seeking authentication. The user must provide a correct response in order to be authenticated. The challenge may take many forms depending on the system. In some systems, it is in the form of a message indicating "unauthorized access" and requesting a password. In other systems, it may be a simple request for a password, a number, a digest, or a nonce (a server specified data string that may be uniquely generated each time a server generates a 401 server error). The person seeking authentication must respond to the system challenge. Nowadays, responses are by a one-way function using a password token, commonly referred to as asynchronous tokens. When the server receives the user response, it checks to be sure the password is correct. If so, the user is authenticated. If not or if for any other reason the network does not want to accept the password, the request is denied.

Challenge-response authentication is used mostly in distributed systems. Though becoming popular, challenge-response authentication is facing challenges as a result of weaknesses that include user interaction and trial-and-error attacks. The problem with user interaction involves the ability of the user to locate the challenge over usually clattered screens. The user then must

quickly type in a response. If a longer than anticipated time elapses, the request may be denied. Based on the degree of security needed, sometimes the user has to remember the long response or sometimes is forced to write it down, and finally the user must transcribe the response and type it in. This is potentially error prone. Some vendors have tried to cushion the user from remembering and typing long strings by automating most of the process either by cut-and-paste of the challenge and responses or through a low-level automated process where the user response is limited to minimum yes/no responses.

In trial-and-error attacks, the intruders may respond to the challenge with a spirited barrage of trial responses hoping to hit the correct response. With powerful computers set to automatically generate responses in a given time frame, it is potentially possible for the intruder to hit on a correct response within the given time frame.

Also of interest is to remember that in its simplest form, challenge-responses that use passwords can be abused because passwords are comparatively easy to steal. And if transmitted in the clear, passwords can also be intercepted. However, this situation is slightly better in the nonce or digest authentication, the more sophisticated of the two forms of scheme, because the password is not sent in the clear over the network. It is encrypted which enhances security, although not fully hack-proof protection.

BIOMETRIC SYSTEM

Biometrics refers to metrics related to human characteristics. Biometrics is a realistic authentication used as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then measurable, distinctive characteristics used to label and describe individuals. Biometric authenticators are frequently labeled as behavioral as well as physiological characteristics. Physiological characteristics are related to the shape of the body. By utilizing biometrics a man could be distinguished in view of "who she/he is" instead of "what she/he has" (card, token, scratch) or "what she/he knows" (secret key, PIN).

As the transaction fraud raises and level of security infringes, the requirement for highly secure identification and personal verification technologies are becoming apparent. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The necessity for biometrics can be found in, state and local governments, federal, in the military, and in commercial applications. Enterprise wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security.

TYPES OF BIOMETRICS

Conventional access methods have their weaknesses – cards can be stolen, pins or keys can be forgotten. Biometric authentication systems use human's biological traits, and so biometric devices can come in any of the forms as illustrated in figure 5.1.

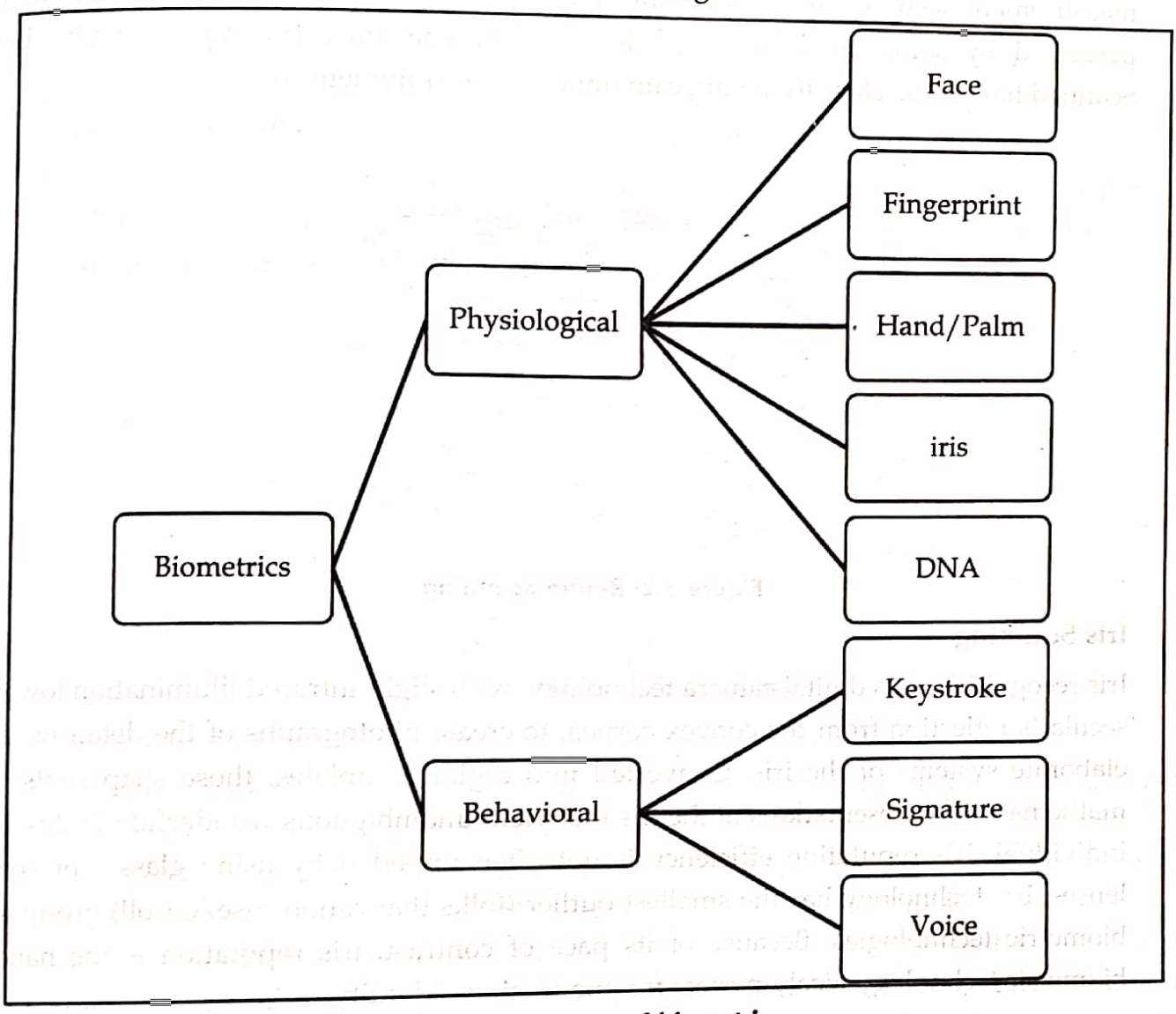

Figure 5.1: Types of biometrics

1. **Retina Scanner**

A retinal scan is a biometric approach that makes use of the unique patterns on someone's retina to discover them. The human retina is a thin tissue composed of neural cells that is located within the posterior part of the eye as shown in figure 5.2. Due to the complex shape of the capillaries that deliver the retina with blood, all and sundry's retina is unique. The network of blood vessels within the retina is so complicated that even identical twins do not proportion a comparable sample. Even though retinal styles can be altered in instance of diabetes, Glaucoma or retinal degenerative disorders, the retina typically remains unaffected from birth till dying. Due to its unique and unchanging nature, the retina seems to be the maximum precise and dependable biometric. Those experiment the unique biometric pattern in every body's iris, and suit it towards a positive range of particular identifying marks that set every person apart from all people else.

Advantages of using Retinal experiment consist of low prevalence of false positives, extraordinarily low (nearly 0%) fake bad charges, highly dependable because no humans have the same retinal sample, rapid results: identity of the issue is verified right away. Dangers include measurement accuracy can be stricken by a sickness such as cataracts, measurement accuracy also can be affected by severe astigmatism, canning technique is perceived by some as invasive, no longer very consumer friendly, difficulty being Scanned have to be close to the dig cam optics, high equipment cost.

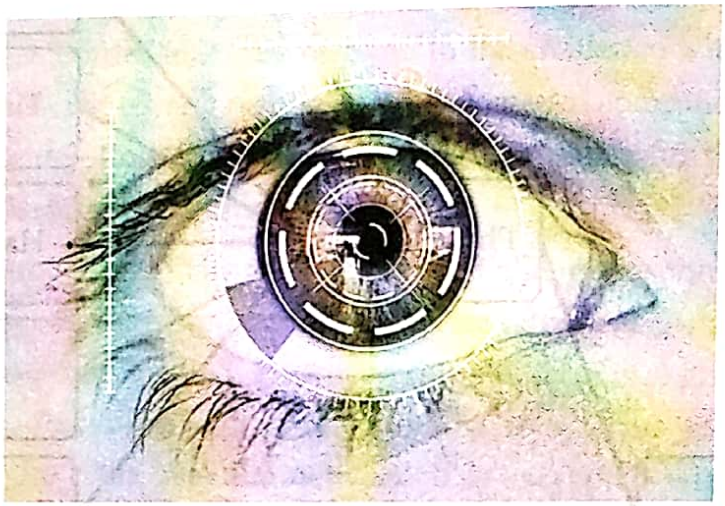

Figure 5.2: Retina Scanning

2. Iris Scanning

Iris recognition uses digital camera technology, with slight infrared illumination lowering secular's reflection from the convex cornea, to create photographs of the detail-wealthy, elaborate systems of the iris. Converted into digital templates, those snap shots offer mathematical representations of the iris that yield unambiguous wonderful identity of an individual. Iris reputation efficiency is not often impeded by using glasses or contact lenses. Iris technology has the smallest outlier (folks that cannot use/enroll) group of all biometric technologies. Because of its pace of contrast, iris reputation is the handiest biometric technology nicely-perfect for one-to-many identity.

Advantage of iris reputation is its balance, or template sturdiness, a single enrollment can clósing an entire life. There are few benefits of the use of iris as biometric identification: it's far an inner organ this is properly included against damage and wear by a rather obvious and touchy membrane (the cornea). This distinguishes it from fingerprints, which may be tough to recognize after years of certain styles of manual labor. The iris is normally flat, and its geometric configuration is handiest managed by complementary muscle groups that manage the diameter of the student. This makes the iris shape far greater predictable than, for example, that of the face.

The iris has a pleasant texture that like fingerprints is determined randomly at some stage in embryonic gestation. Even genetically same individuals have absolutely independent iris textures, while DNA (genetic "fingerprinting") isn't unique for the about 0.2% of the human population who've a genetically same twin. An iris experiment is similar to taking a photograph and can be achieved from about 10 cm to 3 m away. There is no need for

the person to be diagnosed to touch any equipment that has currently been touched by using a stranger, thereby getting rid of an objection that has been raised in some cultures in opposition to fingerprint scanners, in which a finger has to the touch a surface, or retinal scanning, where the eye can be delivered very close to a lens (like looking into a microscope lens).

Even as there are a few clinical and surgical strategies that could affect the coloration and normal form of the iris, the first-rate texture stays remarkably stable over many years. Some iris identifications have succeeded over duration of approximately 30 years. However Iris scanning is a quite new era and is incompatible with the very substantial funding that the law enforcement and immigration government of a few international locations have already made into fingerprint popularity.

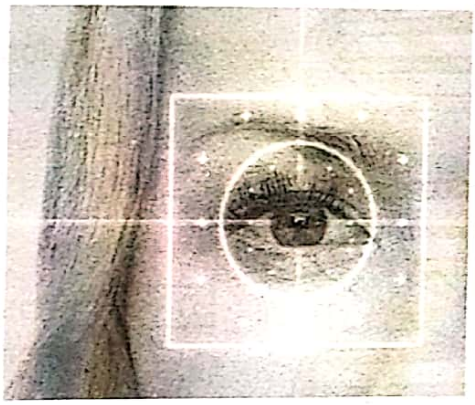

Figure 5.3: Iris Scanning

3. **Finger Print Scanner**

Fingerprints are the graphical glide-like ridges gift on human palms. Finger ridge configurations do no longer exchange for the duration of the life of a person besides due to accidents including bruises and cuts on the fingertips. This belongings makes fingerprints a totally attractive biometric identifier. Fingerprint-based totally private identification has been used for a very long time. As a long way as fee is going, the fingerprint scanning is on the lower stop of the dimensions. The most inexpensive fingerprint scanners are those that best scan the actual print, though the dearer ones really experiment the presence of blood in the fingerprint, the scale and shape of the thumb, and plenty of different features. Those costlier structures in reality capture a 3D photo of the fingerprint, thereby making it a great deal more difficult for the fingerprint to be counterfeited.

Figure 5.4: Finger Print

4. DNA

Not long ago Russian show business was full of rumors that one of the popular Russian singers has two fathers and each father tried his best to influence on the son. Special programmers were created and the situation was discussed but only one thing was interested to public: who was the real father of the singer. The singer himself was confused. In one of the programs the singer and both of his father's decide to take DNA test as shown in figure 5.5.

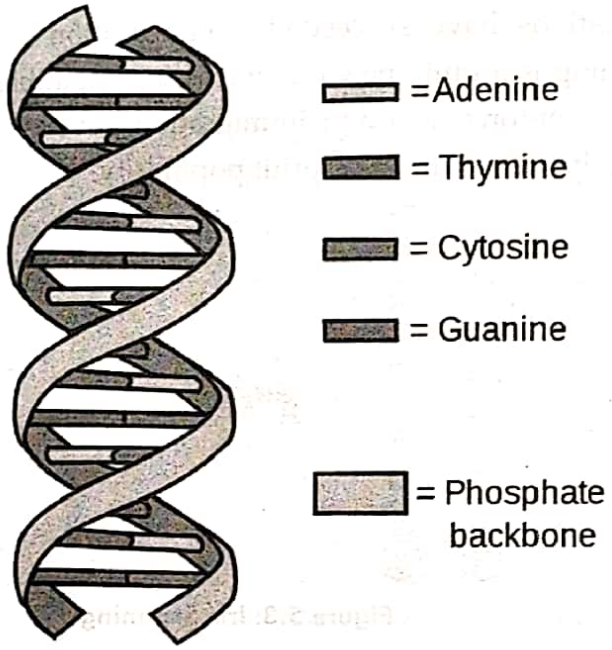

Figure 5.5: Structure of DNA

5. Facial Biometrics

Every individual around the globe has a distinctly unique face, even two twins that the human eye can't differentiate. It might be something as little as the slightly unique placing of the eyebrows, the width of the eyes, or the breadth of the nose. There are sure markers that enable these biometric acknowledgment scanners to in a split second recognize the uniqueness of every individual examining their facial elements, in this manner empowering the gadget to guarantee that lone the single individual with the right bone structure and highlight situation can obtain entrance. PCs have contributed in the programmed acknowledgment of people utilizing the incontestable facial qualities which prompted wide importance of the Face Recognition System (FRS) as shown in figure 5.6.

Figure 5.6: Face recognition system

6. **Voice Recognition**

Each person in the world has a unique voice pattern as shown in figure 5.7, even though the changes are slight and hardly noticeable to the human ear. On the other hand with uncommon voice recognition programming, those moment contrasts in every individual's voice can be noted, experienced and validated to enable the access to the individual that has quality pitch which is a correct one and at the same time voice level also. Surprisingly it can be effective at differentiating two people who have almost identical voice patterns. In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to conclude a conclusive match. Feeding the wrong voice cannot always be avoided in voice recognition as well as the voice capturing machine should be near to the user.

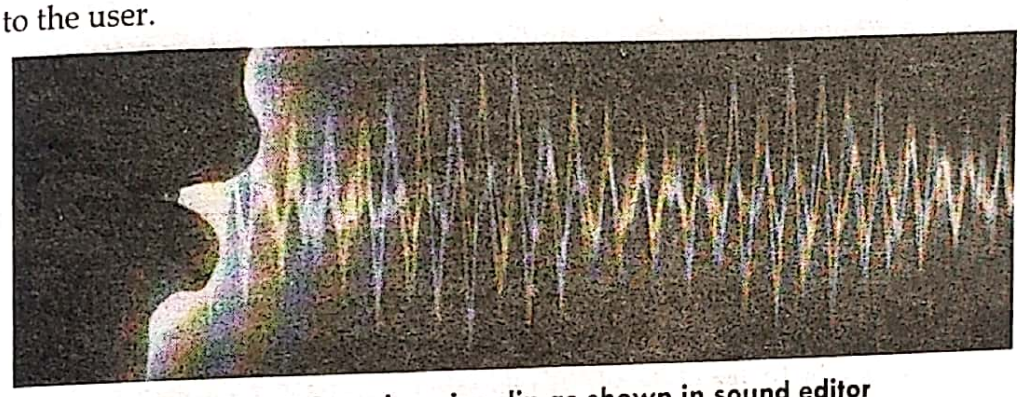

Figure 5.7: Sample voice clip as shown in sound editor

7. **Key Stroke**

Keystroke as shown in figure 5.8, it is the behavior of the human. It means to say that the different humans have the different techniques of pressing keys on such basis the identification takes place. It is 100% software-based, requiring no sensor more than a home computer.

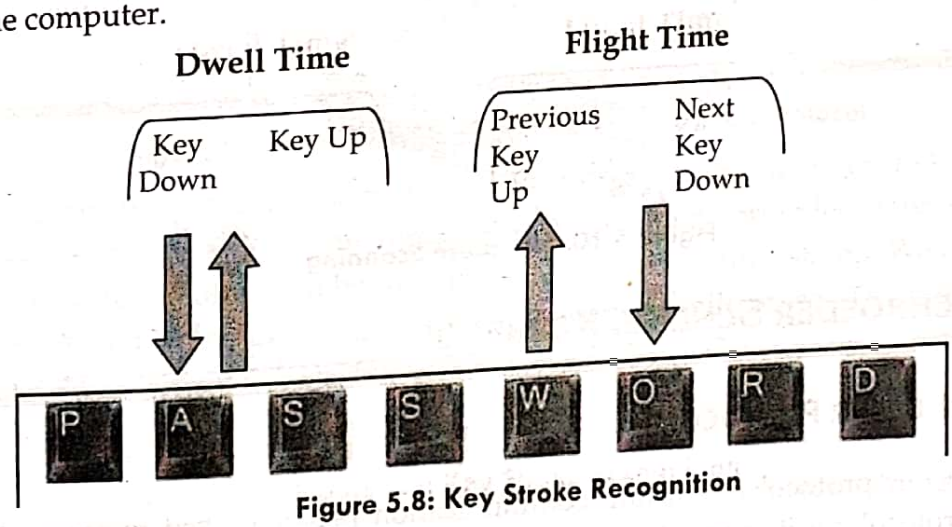

Figure 5.8: Key Stroke Recognition

8. **Hand/ Palm Print Patterns**

By placing your hand on a scanner, you not only have a unique fingerprint pattern, but the size and shape of your entire hand is also very unique as shown in figure 5.9. It differs to a unique finger impression in that it likewise contains other data, for example, touch, indents and symbols which can be utilized when contrasting one palm with

another. Hand prints can be used for criminal, forensic or commercial applications. The main difficulty of hand print is that the print changes with time depending on the type of work the person is doing for an extended duration of time.

Figure 5.9: Hand/Palm-print patterns recognition

9. **Signature Scanning**

Another behavioral biometric is a signature at which the data can be extracted by the signature of that particular person as shown in figure 5.10. The responsibility of a signature is exclusively not only to provide evidence of the identity of the constricting gathering but moderately to provide evidence of deliberation and educated consent signatures can be easily inaccurate With advanced signature capturing devices. Signature recognition correctly became easier and more efficient.

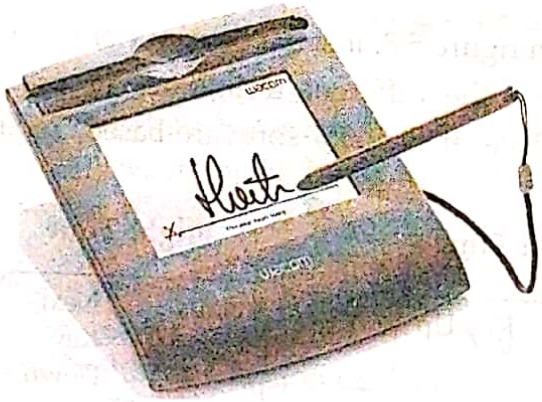

Figure 5.10: Signature Scanning

NEEDHAM-SCHROEDER SCHEME, KERBEROS

NEEDHAM-SCHROEDER PROTOCOL

Needham-Schroeder protocol refers to a communication protocol used to secure an insecure network. The protocol got its name from the creators Roger Needham and Michael Schroeder. This is like a bug-fix to the KDC scheme to eliminate replay attacks. A 3-way handshake (using nonce numbers) very similar to the ubiquitous TCP 3-way handshake is used between communicating parties. A sends a random number R_A to KDC. KDC send back a ticket to A which has the common key to be used.

R_A, R_B and R_{A2} are nonce numbers. R_A is used by A to communicate with the KDC. On getting the appropriate reply from the KDC, **A** starts communicating with **B**, whence another nonce number R_{A2} is used. The first three messages tell B that the message has come from KDC and it has authenticated **A**. The second last message authenticates **B**. The reply from **B** contains R_B, which is a nonce number generated by **B**. The last message authenticates **A**. The last two messages also remove the possibility of replay attack.

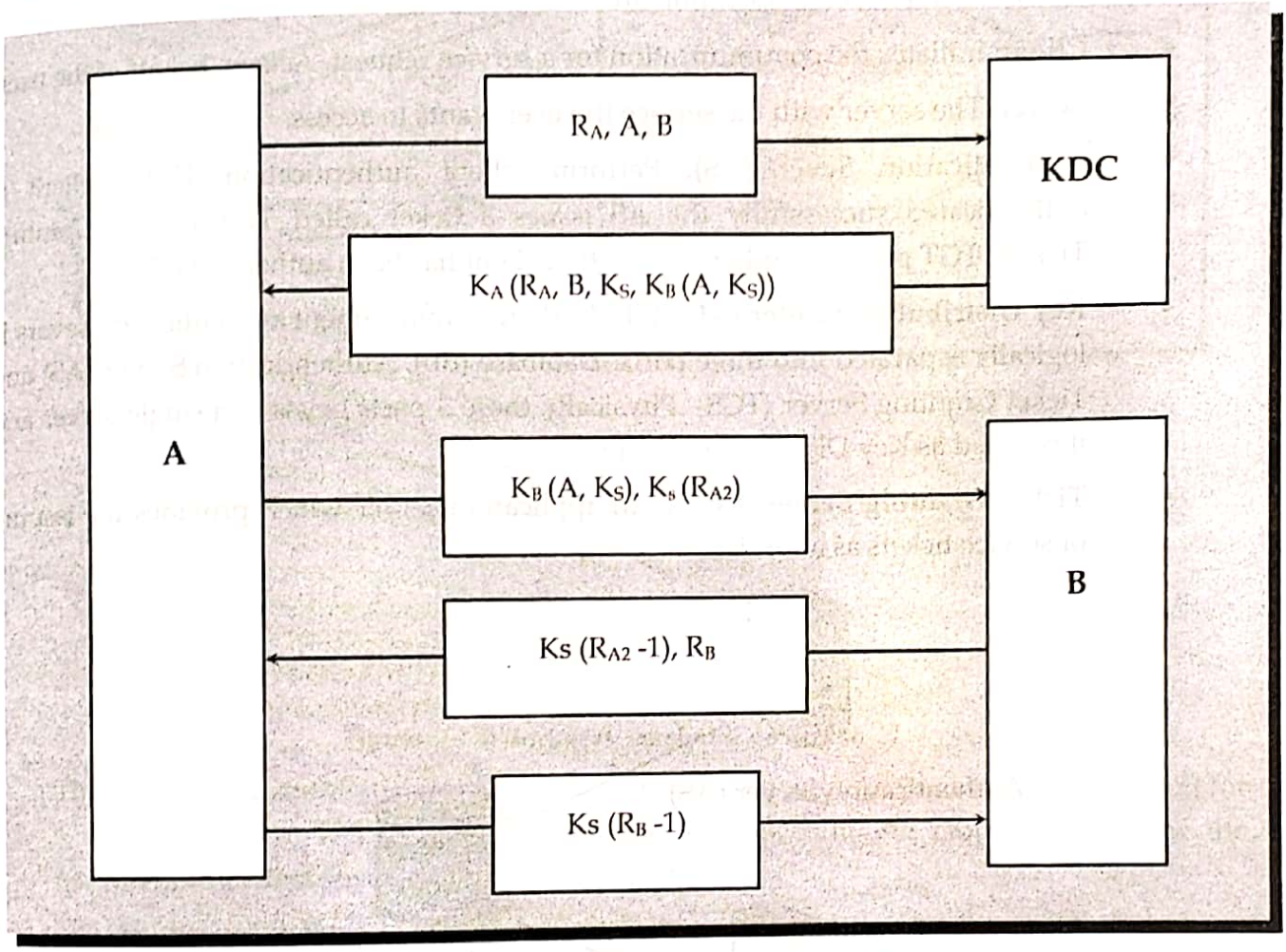

Figure 5.11: Needham-Schroeder Authentication Protocol

However, the problem with this scheme is that if somehow an intruder gets to know the key K_S (maybe a year later), then s/he can replay the entire thing (provided s/he had stored the packets). One possible solution can be that the ticket contains a time stamp. We could also put a condition that **A** and **B** should change the key every month or so. To improve upon the protocol, **B** should also involve KDC for authentication.

KERBEROS

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos is available in many commercial products as well. Kerberos was named after the ferocious three-headed guard dog of Hades appearing in Greek myths. Kerberos was developed by Massachusetts Institute of Technology (MIT) for a project called Athena. A free implementation of this protocol is available from the **Massachusetts Institute of Technology**.

Kerberos authentication is currently the default authorization technology used by Microsoft Windows, and implementations of Kerberos exist in Apple OS, FreeBSD, UNIX, and Linux. Microsoft introduced their version of Kerberos in Windows2000. It has also become a standard for websites and Single-Sign-On implementations across platforms. The **Kerberos Consortium** maintains Kerberos as an **open-source project**. We only discuss version 4, the most popular, and we briefly explain the difference between version 4 and version 5.

Main entities involved in Kerberos operation are:

- **Client:** Initiates the communication for a service request. Acts on behalf of the user.
- **Server:** The server with the service the user wants to access.
- **Authentication Sever (AS):** Performs client authentication. If the client is authenticated successfully the AS issues a ticket called TGT (Ticket Granting Ticket). TGT proves to other servers that client has been authenticated.
- **Key Distribution Center (KDC):** In Kerberos environment authentication severs is logically separated into three parts: Database (db), Authentication Server (AS) and Ticket Granting Server (TGS). Physically these 3 parts exists in a single server and it is called as Key Distribution Center.
- **Ticket Granting Server (TGS):** An application server which provides the issuing of service tickets as a service.

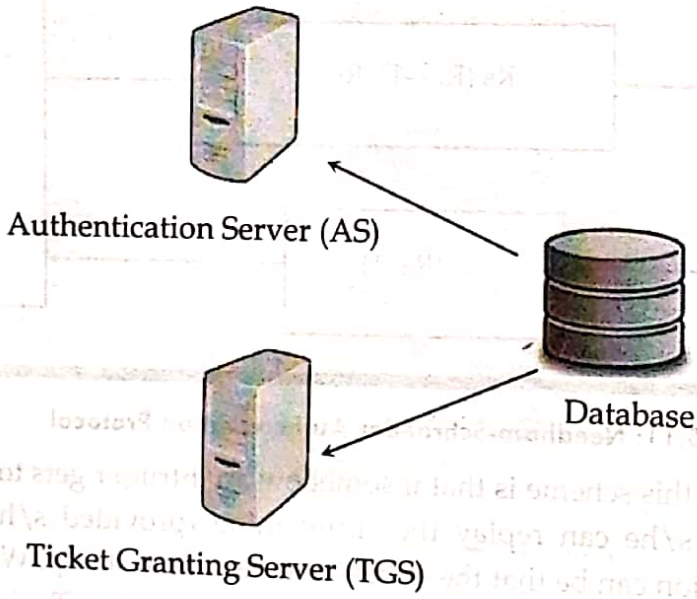

Figure 5.12: Key Distribution Center

In Kerberos operation there are 3 important secret keys. A unique secret key is there for client/user, TGS and server which are shared with the AS.

- **Client/user secret key:** Hash derived by the user's password.
- **TGS secret key:** Hash of the password used to determine TGS.
- **Server secret key:** Hash of the password used to determine the server offering the service.

Kerberos operation steps are explained below and illustrated in figure 5.13.

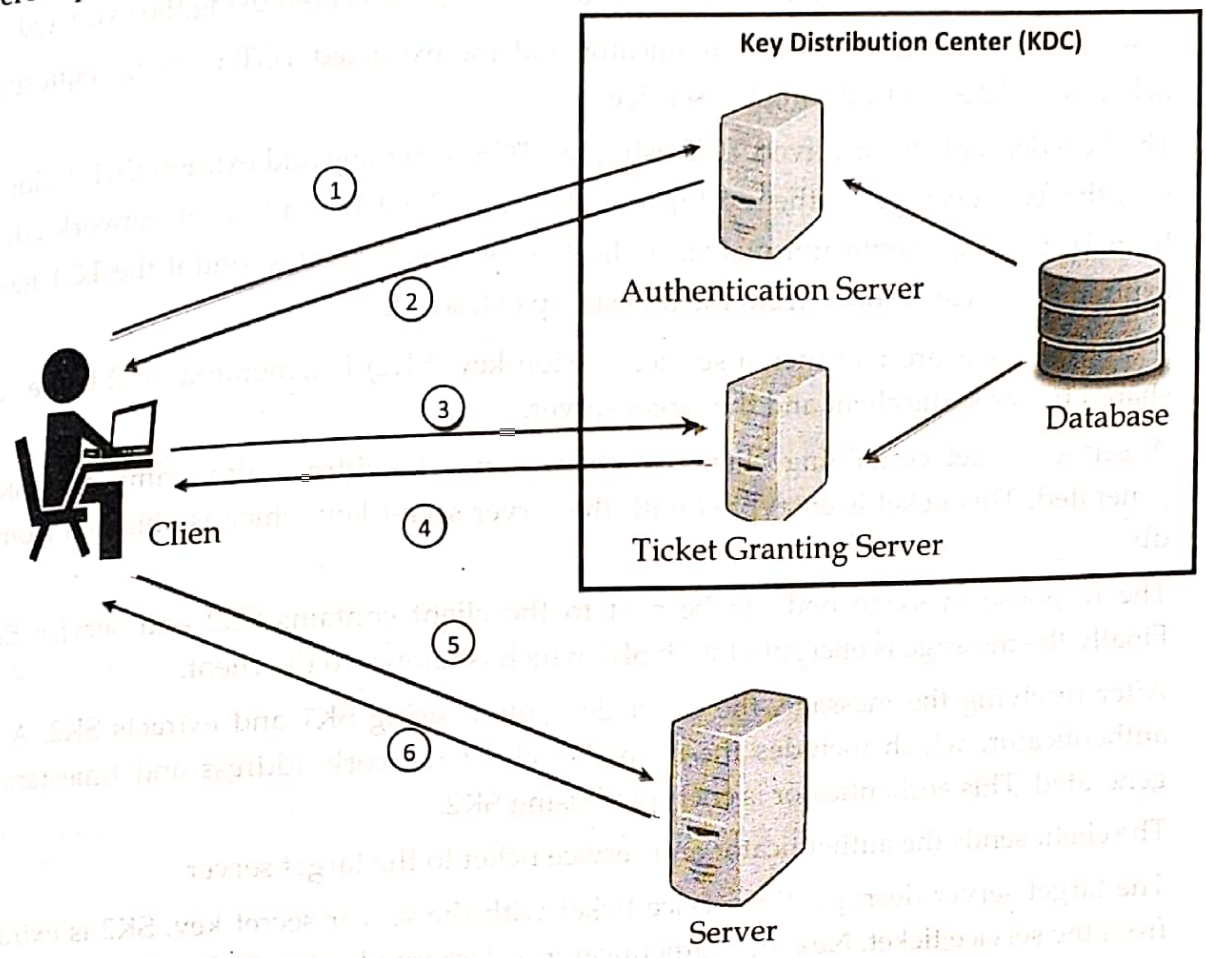

Figure 5.13: Kerberos version 4 operation

1. This is the initial authentication request. The client requests Authentication Sever (AS) for a Ticket Granting Ticket (TGT). The client ID is sent in the request. Note that the password and client/user secret key is not sent.

2. The AS checks for the availability of the client and TGS in the database (db). If either of values is not found, then an error message is sent to the client. If both values are available then the client/user secret key is generated by using the hash of the password of the user. The password of the user is available in the db. Also the TGS secret key is computed. AS generates a session key (SK1) to be shared between the client and the TGS. SK1 is encrypted using the client secret key.

   AS generates a TGT which contains client ID, client network address, lifetime, timestamp, and SK1. The ticket is encrypted with the TGS secret key, so its contents can only be deciphered by the TGS.

   The response message to be sent to client contains of the generated SK1 and TGT. Finally this message body is encrypted with the client/user secret key so that only the client is able to decode the message.

3. Client decrypts the message using its client/user secret key (generated from the password entered by the user) and extracts SK1 and TGT. The authenticator which is

used to validate the client to TGS is generated. The authenticator contains client ID, client network address and client machine timestamp and is encrypted using the extracted SK1.

The client sends the created authenticator and the extracted TGT to TGS, requesting a ticket from the server offering the service.

4. The TGS decrypts the received TGT using the TGS secret key and extracts SK1. Using this key, the TGS decrypts authenticator and checks if client ID and client network address from TGT and authenticator match. A check is also performed to find if the TGT has not expired from. This is done from the timestamp extracted.

   If all the checks are met then a service session key (SK2) is generated. SK2 is the secret shared between the client and the target server.

   A service ticket containing client id, client network address, timestamp and SK2 is generated. This ticket is encrypted with the server secret key which is obtained from the db.

   The response message body to be sent to the client contains SK2 and service ticket. Finally the message is encrypted with SK1 which is known to the client.

5. After receiving the message, the client decrypts it using SK1 and extracts SK2. A new authenticator, which includes the client ID, client network address and timestamp, is generated. This authenticator is encrypted using SK2.

   The client sends the authenticator and service ticket to the target server.

6. The target server decrypts the service ticket with the server secret key. SK2 is extracted from the service ticket. Next the authenticator is decrypted using SK2 and client ID, client network address, timestamp is extracted.

   Checks are performed to verify if client ID and client network address from service ticket and authenticator match. A check is also performed to find that the service ticket has not expired.

   If all checks are met the target server returns a message consisting of the time stamp plus 1, encrypted with SK2 to the client. This message proves that client and the server have completely authenticated each other. Therefore a trusted service session can now begin.

So this is how the Kerberos authentication protocol allows clients to communicate over a network in a secure manner.

KERBEROS VERSION 5

The minor differences between version 4 and version 5 are briefly listed below:

1. Version 5 has longer ticket lifetime.
2. Version 5 allows tickets to be renewed.
3. Version 5 can accept any symmetric-key algorithm.
4. Version 4 uses a different protocol for describing data types.
5. Version 5 has more overhead than version 4.

Table 5.2: Comparison between Kerberos version 4 and version 5

Basis of Comparison	Kerberos Version 4	Kerberos Version 5
Chronology	Kerberos v4 was released prior to the version 5 in the late 1980's.	The version 5 was published in 1993, years after the appearance of version 5.
Key salt algorithm	Uses the principal name partially.	Uses the entire principal name.
Encoding	Uses the "receiver-makes-right" encoding system.	Uses the ASN.1 coding system.
Ticket support	Satisfactory	Well extended. Facilitates forwarding, renewing and postdating tickets.
Network addresses	Contains only a few IP addresses and other addresses for types of network protocols.	Contains multiple IP addresses and other addresses for types of network protocols.
Transitive cross-realm authentication support	No present support for the cause.	Reasonable support present for such authentication.

REALMS

Kerberos allow the global distribution of Ass and TGSs, with each system called a **realm**. A user may get a ticket for a local server or a remote server. In the second case, for example, Alice may ask her local TGS to issue a ticket that is accepted by a remote TGS. The local TGS can issue this ticket if the remote TGS is registered with the local one. Then Alice can use the remote TGS to access the remote real server.

DISCUSSION EXERCISE

1. Authentication is based on three factors. List the factors and discuss why each one determines which type of authentication to use.
2. Making an authentication policy must be a well kept secret to ensure the security of the intended system. Why then is it so important that a security policy include an authentication policy that involves as many as possible? What kind of people must be left out?
3. What do you mean by multiple factors authentication? Discuss the need of MFA.
4. Discuss the types of authentication. List out the some authentication methods.

5. Describe password based authentication in detail.
6. Distinguish between fixed and one-time passwords.
7. What do you mean by dictionary attack? How can it be prevented?
8. Define biometric system. Explain the types of the biometrics.
9. Discuss Needham-Schroeder Protocol in detail.
10. The Kerberos authentication process actually involves two tickets. Explain the need for each ticket and why only one ticket cannot be used.
11. Discuss in detail the role played by each one of the five players in a Kerberos authentication process.
12. Does Kerberos protocol ensures authentication and confidentiality in secure system? Explain.
13. In Kerberos, when Bob receives a ticket from Alice, how does he know it came from Alice?

❑❑❑