UNIT V

AUTHENTICATION

CONTENTS

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

AUTHENTICATION

- *Authentication is the binding of an identity to a principal/subject.*
- *The external entity must provide information to enable the system to confirm its identity.*

AUTHENTICATION BASICS

This information comes from one (or more) of the following(Verification categories)

- *What the entity knows (such as passwords or secret information)*
- *What the entity has (such as a badge or card)*
- *What the entity is (such as fingerprints or retinal characteristics)*
- *Where the entity is (such as in front of a particular terminal)*

AUTHENTICATION BASICS

- *The authentication process consists of obtaining the authentication information from an entity, analyzing the data, and determining if it is associated with that entity.*
- *This means that the computer must store some information about the entity. It also suggests that mechanisms for managing the data are required.*
- These requirements in an *authentication system* consisting of five components

AUTHENTICATION SYSTEM AND COMPONENTS

1. The set A of *authentication information* is the set of specific information with which entities prove their identities.
2. The set C of *complementary information* is the set of information that the system stores and uses to validate the authentication information.
3. The set F of *complementation functions* that generate the complementary information from the authentication information.

   That is, for $f \in F$, $f: A \rightarrow C$.

AUTHENTICATION SYSTEM AND COMPONENTS

4. The set L of authentication functions that verify identity. That is, for $l \in L$, $l: A \times C \rightarrow \{$ ***true***, ***false*** $\}$.

5. The set S of selection functions that enable an entity to create or alter the authentication and complementary information

EXAMPLE

A user authenticates himself by entering a password, which the system compares with the cleartext passwords stored online. Here, A is the set of strings making up acceptable passwords, $C = A$, $F = \{ I \}$, and $L = \{$ **eq** $\}$, where I is the identity function and **eq** is **true** if its arguments are the same and **false** if they are not.

PASSWORDS

- A *password* is information associated with an entity that confirms the entity's identity.
- Passwords are an example of an authentication mechanism based on what people know: the user supplies a password, and the computer validates it. If the password is the one associated with the user, that user's identity is authenticated. If not, the password is rejected and the authentication fails.

PASSWORDS

- The simplest password is some sequence of characters. In this case, the *password space* is the set of all sequences of characters that can be passwords.
- EXAMPLE:
- One installation requires each user to choose a sequence of 10 digits as a password. Then A has 1010 elements (from “0000000000” to “9999999999”).

PASSWORDS

- The simplest and Oldest method of entity authentication.
- Each user has a user identification that is public , and a password that is private.
- The scheme can be divided into two groups: the fixed password and one-time password.

FIXED PASSWORDS

- A password that is used over and over again for every access.

Different Approaches:

Approach 1:the system keeps table (a file) , that is sorted by user identification. To access the system resource, the user sends her user Id and password , in plaintext, to system, if matches the password in table, access is granted. (Attacks on first approach)

Approach 2: Store hash of the Password.

FIXED PASSWORDS

- Dictionary Attack:

The hash function prevents intruder from gaining access to system even though she has the password file.

DICTIONARY ATTACK

- The name of this attack comes from the list of words (a “dictionary”) used for guesses. The dictionary may be a set of strings in random order or (more usually) a set of strings in decreasing order of probability of selection.
- If the complementary information and complementation functions are available, the dictionary attack takes each guess g and computes $f(g)$ for each $f \in F$. If $f(g)$ corresponds to the complementary information for entity E, then g authenticates E under f. This is a *dictionary attack type 1*.
- If either the complementary information or the complementation functions are unavailable, the authentication functions $l \in L$ may be used. If the guess g results in l returning **true**, g is the correct password. This is a *dictionary attack type 2*.

EXAMPLE

- Attackers often obtain a UNIX system's password file and use the (known) complementation function to test guesses. (Many programs such as *crack* automate this process.) This is a type 1 attack. But the attackers need access to the system to obtain the complementation data in the password file. To gain access, they may try to guess a password using the authentication function. They use a known account name (such as *root*) and guess possible passwords by trying to log in. This is a type 2 attack

CHALLENGE-RESPONSE

- Passwords have the fundamental problem that they are *reusable*. If an attacker sees a password, she can later *replay* the password. The system cannot distinguish between the attacker and the legitimate user, and allows access.
- An alternative is to authenticate in such a way that the transmitted password changes each time. Then, if an attacker replays a previously used password, the system will reject it.

DEFINITION

- *Let user U desire to authenticate himself to system S. Let U and S have an agreed-on secret function f. A challenge-response authentication system is one in which S sends a random message m (the challenge) to U, and U replies with the transformation r = f(m) (the response). S validates r by computing it separately.*

BIOMETRICS

- *Biometrics is the automated measurement of biological or behavioral features that identify a person.*
- *Biometrics represent the "something you are" method of authentication .*
- *Whenever the user accesses the system, the biometric authentication mechanism verifies the identity.*

BIOMETRICS

- This is considerably easier than identifying the user because no searching is required. A comparison to the known data for the claimed user's identity will either verify or reject the claim.
- There are many different types of biometrics, including such long-established methods as fingerprints. Recently, biometrics based on speech recognition, gait (walking) recognition, and even a digital doggie (odor recognition) have been developed.
- Common characteristics are fingerprints, voice characteristics, eyes, facial features, and keystroke dynamics.

AN IDEAL BIOMETRIC WOULD SATISFY ALL OF THE FOLLOWING:

- **Universal** — A biometric should apply to virtually everyone. In reality, no biometric applies to everyone. For example, a small percentage of people do not have readable fingerprints.
- **Distinguishing** — A biometric should distinguish with virtual certainty.
- **Permanent** — Ideally, the physical characteristic being measured should never change. In practice, it's sufficient if the characteristic remains stable over a reasonably long period of time

AN IDEAL BIOMETRIC WOULD SATISFY ALL OF THE FOLLOWING:

- **Collectable** — The physical characteristic should be easy to collect without any potential to cause harm to the subject. In practice, collectability often depends heavily on whether the subject is cooperative or not.

- Reliable, robust, and user-friendly.

PHASES TO A BIOMETRIC SYSTEM

- First, there is an ***enrollment phase***, where subjects have their biometric information gathered and entered into a database. Since this is one-time work (per subject), it's acceptable if the process is slow and multiple measurements are required.
- The second phase in a biometric system is the ***recognition phase***. This occurs when the biometric detection system is used in practice to determine whether (for the authentication problem) to authenticate the user or not. This phase must be quick, simple, and accurate.

TYPES OF ERRORS/ACCURACY

There are two types of errors that can occur in biometric recognition.

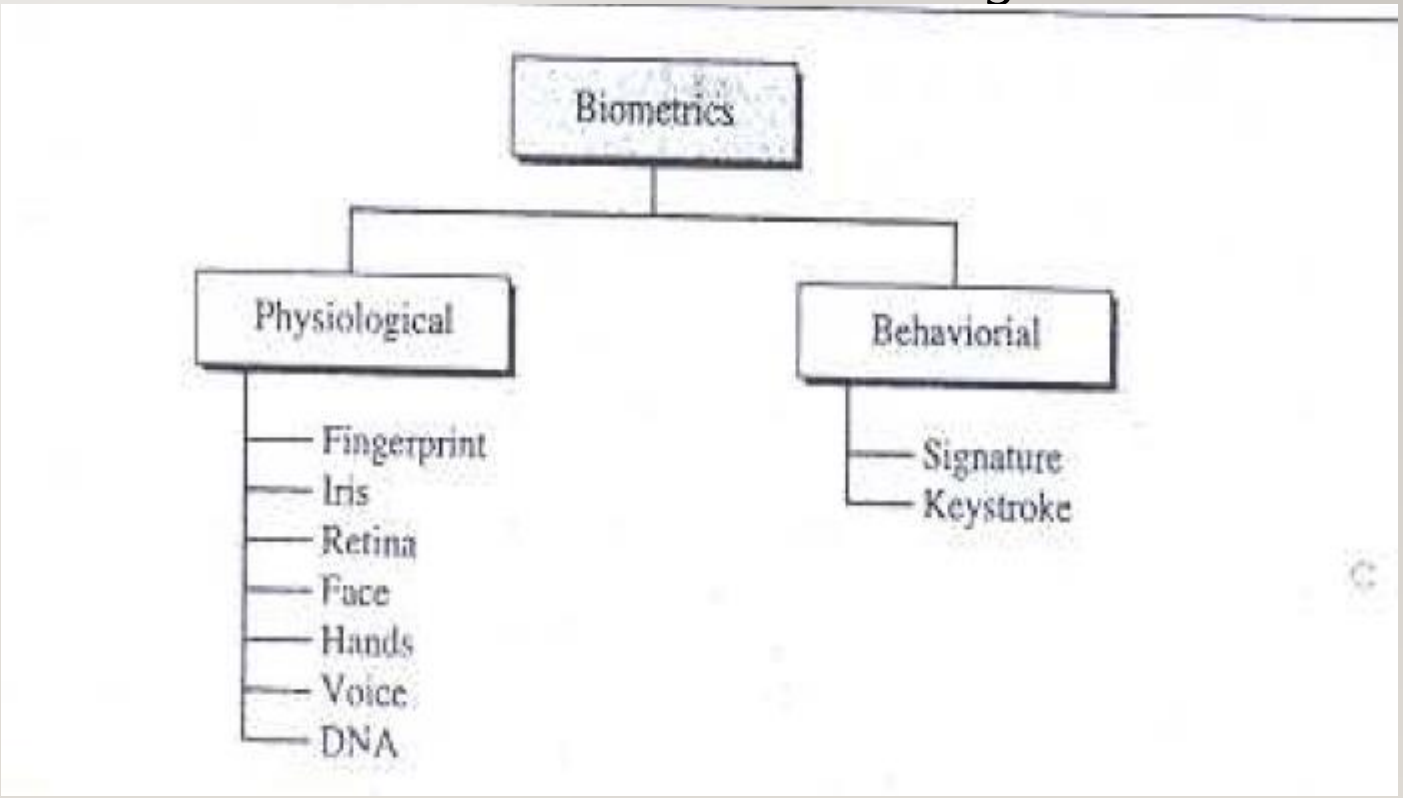
- *Suppose Bob poses as Alice and the system mistakenly authenticates Bob as Alice. The rate at which such mis authentication occurs is the* ***fraud rate****. (False Acceptance Rate-FAR).* ***It is measured as the False acceptance to the total number of attempts. (in percentage)***
- *Now suppose that Alice tries to authenticate as herself, but the system fails to authenticate her. The rate at which this type of error occurs is the* ***insult rate(False Rejection Rate). It is measured as False rejection to the total number of attempts. (in percentage)***

- *The **equal error rate** is the rate for which the fraud and insult rates are the same. That is, the parameters of the system are adjusted until the fraud rate and insult rate are precisely in balance.*

BIOMETRIC EXAMPLES

Biometric techniques can be divided into two broad categories: physiological and behavioral.

- *Physiological measures physical traits of human body for verification and Identification.*
- *However behavioral measures human behavior traits.*



FINGERPRINTS

- A fingerprint biometric works by first capturing an image of the fingerprint. The image is then enhanced using various image-processing techniques, and various points are identified and extracted from the enhanced image as shown in fig.

Figure 7.2: Automatic Extraction of Minutia

- The points extracted by the biometric system are compared in a manner that is somewhat analogous to the manual analysis of fingerprints.
- For authentication, the extracted points are compared with the claimed user's stored information, which was previously captured during the enrollment phase. The system then determines whether a statistical match occurs, with some predetermined level of confidence.

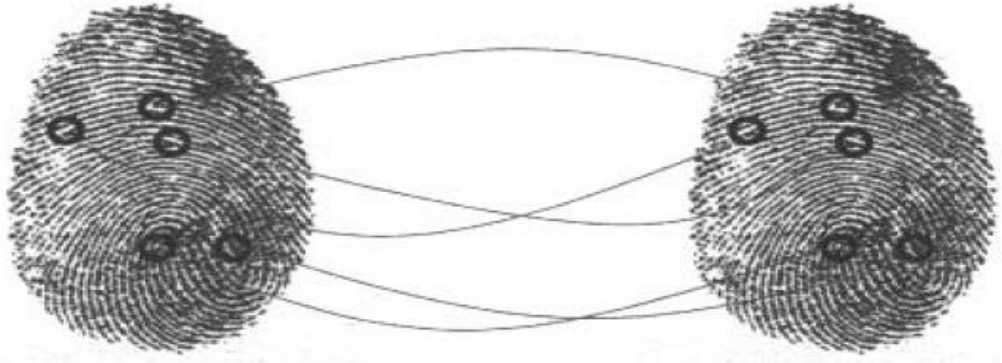


Figure 7.3: Minutia Comparison

HAND GEOMETRY

- The shape of the hand is carefully measured, including the width and length of the hand and fingers.
- Human hands are not nearly as unique as fingerprints, but hand geometry is easy and quick to measure, while being sufficiently robust for many authentication uses.
- One advantage of hand geometry systems is that they are fast, taking less than one minute in the enrollment phase and less than five seconds in the recognition phase. Another advantage is that human hands are symmetric, so if the enrolled hand is, say, in a cast, the other hand can be used by placing it palm side up. Some disadvantages of hand geometry include that it cannot be used on the young or the very old.

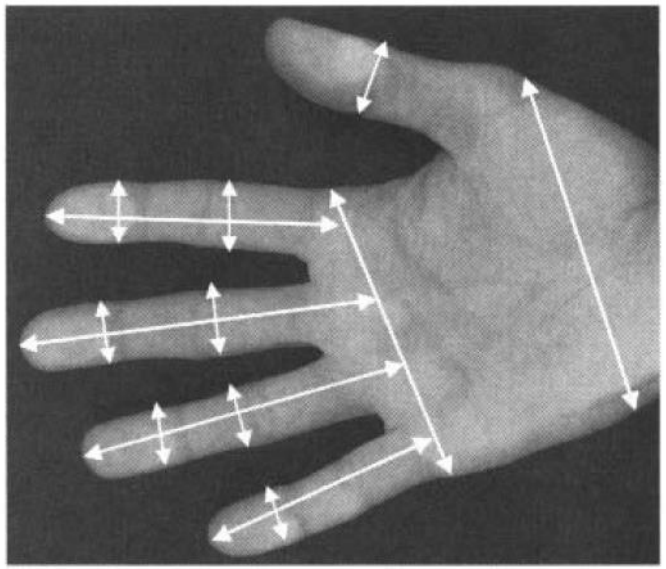


Figure 7.4: Hand Geometry Measurements

IRIS SCAN

- one of the best for authentication is the iris scan. The development of the iris (the colored part of the eye) is chaotic, which implies that minor variations lead to large differences. There is little or no genetic influence on the iris pattern, so that the measured pattern is uncorrelated for identical twins and even for the two eyes of one individual.
- Another desirable property is that the pattern is stable throughout a lifetime

- Iris scan systems require sophisticated equipment and software. First, an automated iris scanner locates the iris. Then a black and white photo of the eye is taken. The resulting image is processed using a two-dimensional wavelet transform, the result of which is a 256-byte (that is, 2048-bit) iris code.
- Two iris codes are compared based on the Hamming distance between the codes. Suppose that Alice is trying to authenticate using an iris scan. Let x be the iris code computed from Alice's iris in the recognition phase, while y is Alice's iris code stored in the scanner's database, which was gathered during the enrollment phase.

- Then *x* and *y* are compared by computing the distance *d(x, y)* defined by

$$d(x, y) = \frac{\text{number of non-match bits}}{\text{number of bits compared}}.$$

For example, d(0010,0101) = 3/4

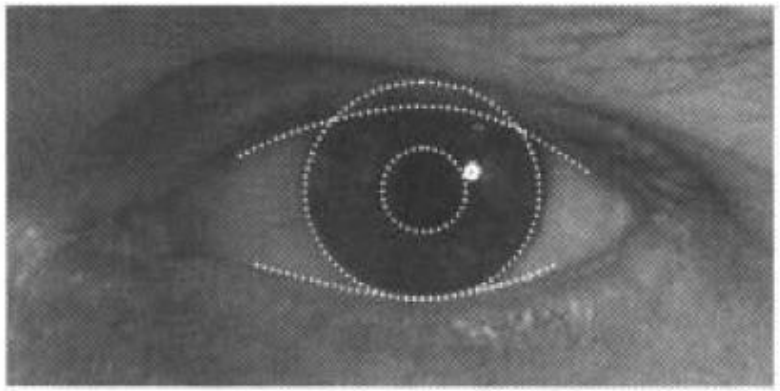


Figure 7.5: An Iris Scan

APPLICATIONS OF BIOMETRIC

- *Access to facilities*
- *Access to Information systems.*
- *Law Enforcement: Investigation using fingerprint and DNA , forensic analysis.*
- *Boarder Control and immigration Control.*

TWO-FACTOR AUTHENTICATION

- Any authentication method that requires two out of the three "somethings" is known as *two-factor authentication.* Another example of a two-factor authentication is an ATM card, where the user must have the card and know the PIN number.
- Other examples of two-factor authentication include a credit card together with a signature, a biometric thumbprint system that also requires a password, and a cell phone that requires a PIN

NEEDHAM–SCHROEDER PROTOCOL

- is a cryptographic protocol designed to establish secure communication between two parties over an insecure network.
- It was proposed by Roger Needham and Michael Schroeder in 1978 and has since become a fundamental protocol in network security.
- Its goal is to establish a shared session key between initiator and responder, which can be used for secure communication.
- N-S is a shared-key authentication protocol designed to generate and propagate a session key, i.e., a shared key for subsequent symmetrically encrypted communication.
- The Needham–Schroeder Symmetric Key Protocol, based on a symmetric encryption algorithm. It forms the basis for the Kerberos protocol. This protocol aims to establish a session key between two parties on a network, typically to protect further communication.

NEEDHAM–SCHROEDER PROTOCOL

- The *Needham–Schroeder Symmetric Key Protocol*, based on a symmetric encryption algorithm. It forms the basis for the Kerberos protocol. This protocol aims to establish a session key between two parties on a network, typically to protect further communication.
- The *Needham–Schroeder Public-Key Protocol*, based on public-key cryptography. This protocol is intended to provide mutual authentication between two parties communicating on a network

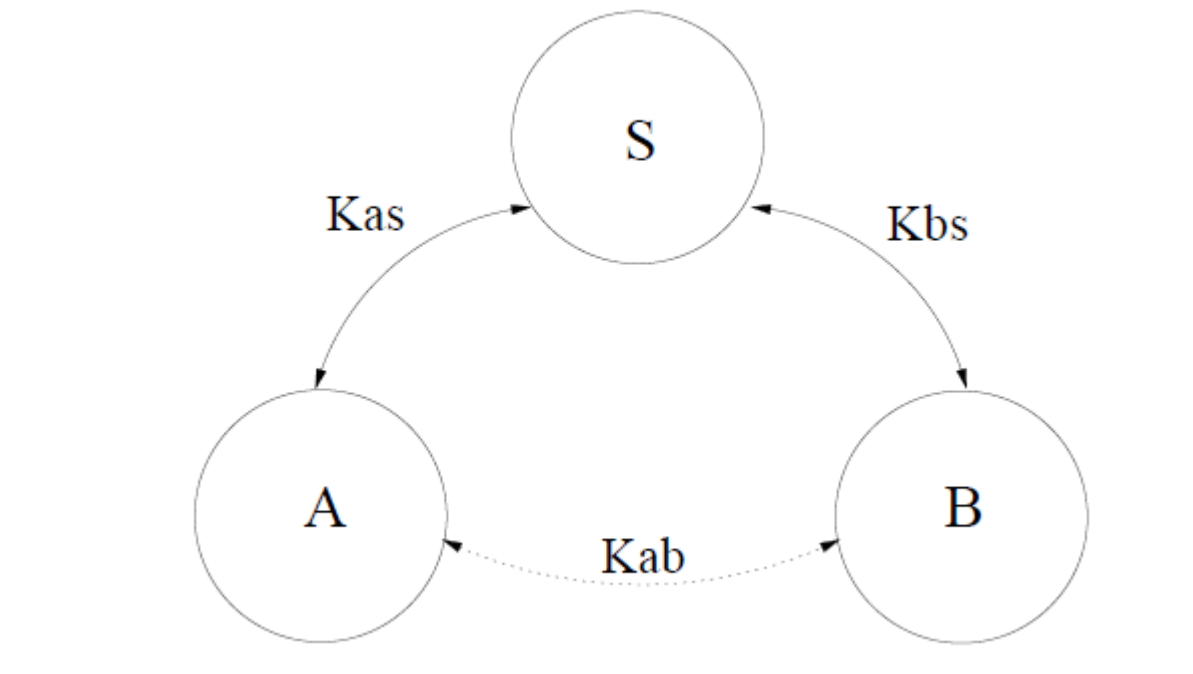
ASSUMPTIONS OF NEEDHAM-SCHROEDER

- There are three principals: A and B, two principals desiring mutual communication, and S, a trusted key server.
- Here, Alice (A) initiates the communication to Bob (B). S is a server trusted by both parties.
- In the communication: A and B are identities of Alice and Bob respectively.
- K_{AS} is a symmetric key known only to A and S
- K_{BS} is a symmetric key known only to B and S

ASSUMPTIONS OF NEEDHAM-SCHROEDER

- N_A and N_B are nonces (short for “numbers used once”) generated by A and B respectively
- K_{AB} is a symmetric, generated key, which will be the session key of the session between A and B

NEEDHAM-SCHROEDER PROTOCOL



NEEDHAM-SCHROEDER PROTOCOL

1. $A \mid\!\!\longrightarrow S : A, B, N_a$
2. $S \longrightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \longrightarrow B : \{K_{ab}, A\}_{K_{bs}}$
4. $B \longrightarrow A : \{N_b\}_{K_{ab}}$
5. $A \longrightarrow B : \{N_b - 1\}_{K_{ab}}$

NEEDHAM-SCHROEDER PROTOCOL

1. Alice includes her identity (A), Bob's identity (B), and a random nonce (Na) to identify the session.
2. Upon receiving Alice's request, the trusted server (S) encrypts the message using the shared key K_{as}, ensuring that only Alice can read it. Alice recognizes her nonce (N_a) and assumes the response is fresh. She obtains the session key (K_{ab}) and receives the ticket $\{K_{ab}, A\}K_{bs}$. However, Alice cannot read or modify the ticket as it is protected by the key K_{bs}, which Alice cannot decrypt.
3. Alice forwards the ticket $\{K_{ab}, A\}K_{bs}$ to Bob, allowing him to decrypt the ticket and learn that Alice (A) wishes to establish communication with him. Bob also obtains the session key K_{AB}.

NEEDHAM-SCHROEDER PROTOCOL

4. Bob responds by sending a nonce (N_b) to Alice, encrypted with the session key K_{ab}. Although Alice is unaware of N_b, she recognizes K_{ab} as the new session key, indicating that Bob possesses the knowledge of the shared key.

5. To ensure authenticity, Alice sends a modified nonce (N_b-1) to Bob, encrypted with the new session key K_{ab}. By knowing that only Alice possesses N_b, Bob confirms the origin of the message. The change from N_b to N_b-1 differentiates messages sent in steps 4 and 5, preventing replay attacks.

6. Alice and Bob have now established a secure connection and can communicate safely using their session key K_{ab}.

ATTACKS ON THE PROTOCOL

- The protocol is vulnerable to a replay attack .If an attacker uses an older, compromised value for K_{AB}, he can then replay the message $\{ K_{AB}, A \} K_{BS}$ to Bob who will accept it, being unable to tell that the key is not fresh.

KERBEROS

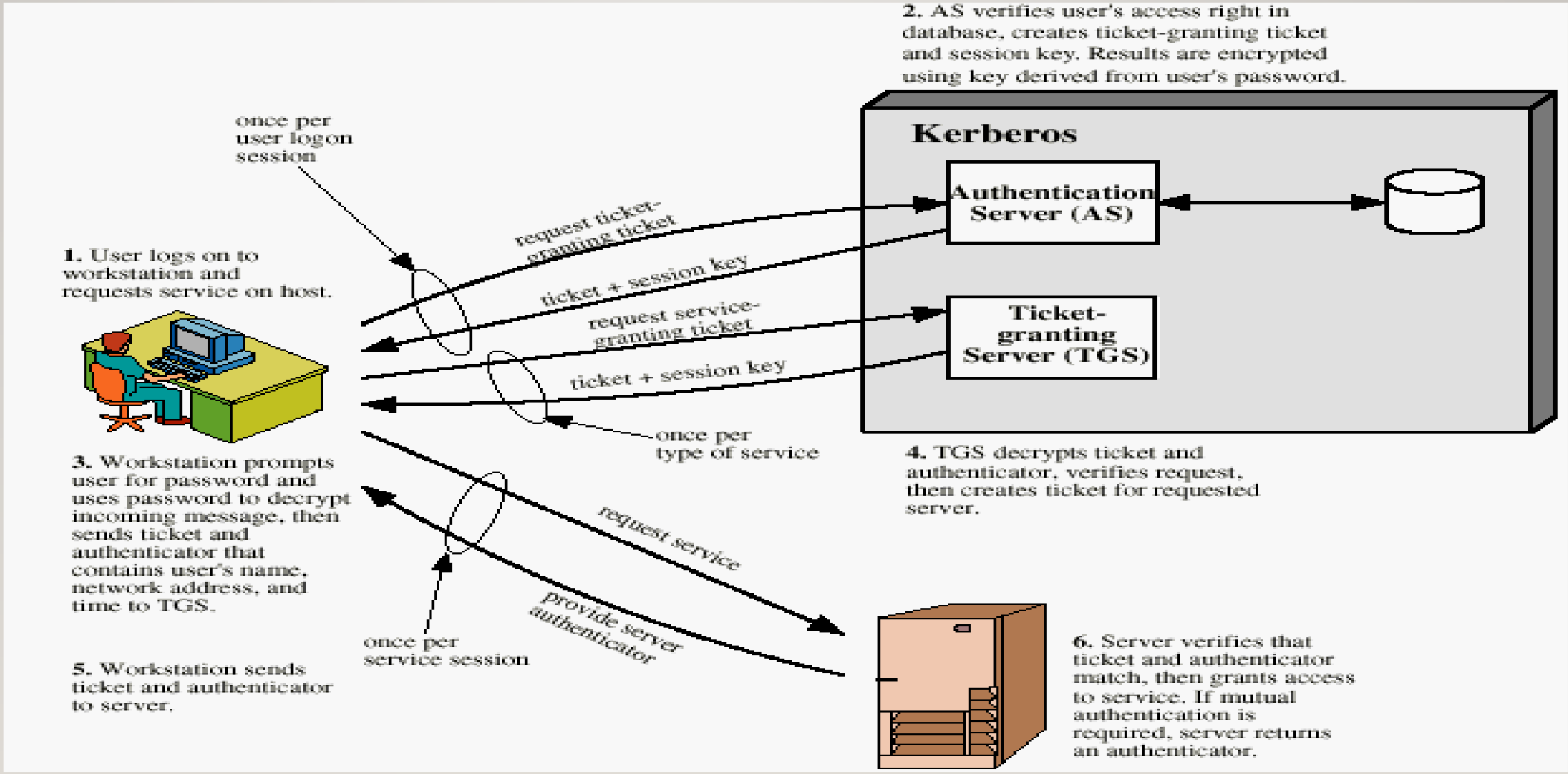
- Implement the idea of Needham-Schroeder protocol
- Kerberos is a **network authentication protocol**
- Provides authentication and secure communication
- Relies entirely on **symmetric cryptography**
- Developed at MIT: two versions, Version 4 and Version 5 (specified as RFC1510)
- http://web.mit.edu/kerberos/www
- Used in many systems, e.g., Windows 2000 and later as default authentication protocol

KERBEROS OVERVIEW

- One issue of Needham-Schroeder
  - Needs the key each time a client talks with a service
- Solution: Separates TTP into an AS and a TGT.
- The client authenticates to AS using a long-term *shared secret* and receives a TGT.
  - supports single sign-on
- Later the client can use this TGT to get additional tickets from TGS without resorting to using the shared secret. These tickets can be used to prove authentication to SS.

AS = Authentication Server
SS = Service Server
TGS = Ticket Granting Server
TGT = Ticket Granting Ticket

OVERVIEW OF KERBEROS



KERBEROS DRAWBACK

- Single point of failure:
  - requires online Trusted Third Party: Kerberos server
- Security partially depends on tight clock synchronization. Convenience requires loose clock synchronization
  - Use timestamp in the protocol
  - The default configuration requires synchronization to with 10 minutes.
- Useful primarily inside an organization
  - Does it scale to Internet? What is the main difficulty?

TASK

- Differentiate between Entity Authentication and data-origin authentication.
- Explain Needham Schroeder public key protocol.