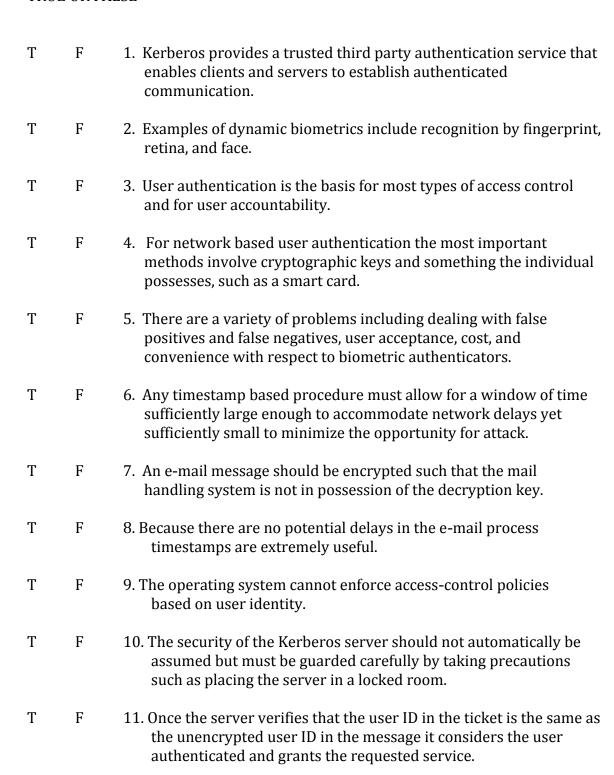
USER AUTHENTICATION PROTOCOLS

TRUE OR FALSE



F

T

MULT	IPLE CHOICE		
1.	is an authentication service designed for use in a distributed environment.		
	A. Kerberos	B. PCBC	
	C. Toklas	D. X.509	
2.	2. The approach is unsuitable for a connectionless type of applicate because it requires the overhead of a handshake before any connectionle transmission, effectively negating the chief characteristic of a connection transaction.		
	A. timestamp	B. backward reply	
	C. challenge-response	D. replay	
3.	A common item of authentication inform	ation associated with a user is a	
	A. nonce	B. timestamp	
	C. ticket	D. password	
4.	The overall scheme of Kerberos is that of a trusted third party authentication service that uses a protocol based on a proposal by		
	A. Needham and Schroeder	B. Kehn	
	C. Denning	D. Gong	

12. It is the ticket that proves the client's identity.

5.	is a procedure that allows communicating parties to verify that the contents of a received message have not been altered and that the source is authentic.		
	A. Identification	B. Message authentication	
	C. Verification	D. User authentication	
6.	. Presenting an identifier to the security system is the step.		
	A. authentication	B. verification	
	C. identification	D. clarification	
7.	Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the step.		
	A. identification	B. verification	
	C. clarification	D. authentication	
8.	The is unsuitable for a connectionless type of application becaus requires the overhead of a handshake before any connectionless transmission effectively negating the chief characteristic of a connectionle transaction.		
	A. timestamp approach	B. challenge-response approach	
	C. simple replay approach	D. one-way authentication approach	
9.	Kerberos relies exclusively on	·	
	A. symmetric encryption	B. asymmetric encryption	
	C. private key encryption	D. public key encryption	
10	. A Kerberos is a set of ma	naged nodes that share the same Kerberos	

	A. realm	B. TGS	
	C. network	D. principal	
11	. In an unprotected network e for service. The obvious secu	nvironment any client can apply to any server urity risk of this is	
	A. certification	B. authentication	
	C. impersonation	D. authorization	
12		m of minimizing the number of times that a user the risk of an eavesdropper capturing the wn as the	
	A. authentication server	B. ticket granting server	
	C. Kerberos mutual authenti	cation D. PCBC mode	
SHOR	T ANSWER		
1.	protocols enable communicating parties to satisfy themselves mutually about each other's identity and to exchange session keys.		
2.	in Greek mytholog guards the entrance of Hades	y is a three headed dog with a serpent's tail that s.	
3.	There are four general means of authenticating a user's identity. They are: something the individual knows, something the individual possesses, something the individual is, and something the individual		
4.	To convince the server that a user is authentic, the authentication server creates a that contains the user's ID and network address and the server's ID and sends it back to the client so they can continue the request for service.		
5.	An authentication process co	onsists of two steps: identification step and	
6.	<u>-</u>	Kerberos listed the following requirements:	

7.	Examples of something the individual possesses would include cryptographic keys, electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a
8.	The is responsible for generating keys to be used for a short time over a connection between two parties and for distributing those keys using the master keys to protect the distribution.
9.	A is where an opponent intercepts a message from the sender and replays it later when the timestamp in the message becomes current at the recipient's site.
10.	is an authentication service developed as part of Project Athena at MIT.
11.	A solution, which eliminates the burden of each server having to confirm the identities of clients who request service, is to use an that knows the passwords of all users and stores these in a centralized database and shares a unique secret key with each server.
	The ticket granting ticket is encrypted with a secret key known only to the AS and the
_	on 1. When you request a service via Kerberos you are presented with a What does the ticket contain and how is it used?
_	on 2. Does message authentication imply user authentication? Is the opposite xplain your answer.

Question 3. Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

- a) John peeks at Alice's password when she is logging in.
- b) John logs into Alice's account using Alice's password without Alice knowing about it.
- c) There is a process running in Alice's machine, which is updating a database from a remote machine. John interrupts the process, results in inconsistent databases.
- d) John copies a file from Alice's account and then deletes the file from Alice's directory.

Question 4. Classify each of the following as a violation of confidentiality, of integrity, of availability, or non-repudiation

- a) Alice copies Bob's homework.
- b) Alice crashes Bob's operating system.
- c) Alice changes the amount on Bob's check from 100 to 1000.
- d) Alice does not honor the contract between her and Bob.