KERBEROS: OVERVIEW

COMPUTER SYSTEMS SECURITY

GORDON | REYNOLDS (2019)

1

TODAY ….

Today we will overview Kerberos, a server/client security protocol.

GORDON | REYNOLDS (2019)

2

COMPUTER SYSTEMS SECURITY

KERBEROS: OVERVIEW

GORDON | REYNOLDS (2018)

3

OVERVIEW

- Kerberos is a client/server authentication protocol based on a ticketing system.
- In most computer systems, a user typically proves their identity by providing a password.
- Their password is then sent via an untrusted network to the authentication servers for verification.
- It is therefore necessary to prevent anyone from eavesdropping on the users password, as knowing their password allows anyone to assume that users identify within the IT environment.

GORDON | REYNOLDS (2018)

4

OVERVIEW

- In addition, it is also necessary to provide a means of authenticating users to use any service available on the network at anytime.
  - Such as, file shares, printers, management servers …. Etc
  - Kerberos provides authentication. It ***doesn't*** provide authorisation or accounting services.
- This can be achieved with Kerberos, which was designed for two main purposes:
  - Security
  - Authentication

GORDON | REYNOLDS (2018)

5

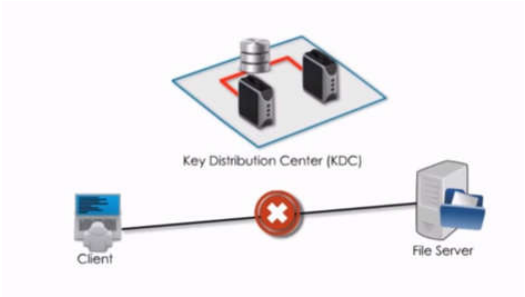
COMPUTER SYSTEMS SECURITY

KERBEROS: OPERATION

GORDON | REYNOLDS (2018)

6

KERBEROS PROCESS:

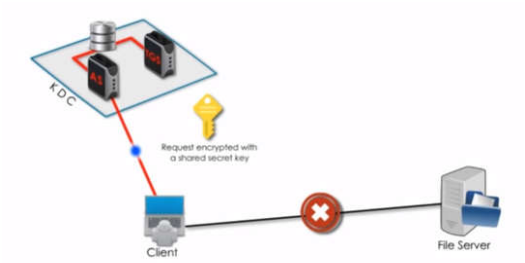


- Suppose a client wants to access a file server, with Kerberos, the client must be verified through a trusted third-party.
- This trusted third party is called a, **Key Distribution Centre** (KDC)

GORDON | REYNOLDS (2018)

7

KERBEROS PROCESS:

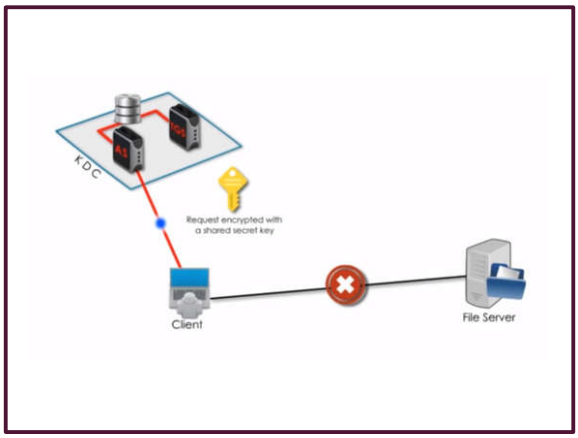


- The Key Distribution Centre (KDC) consists of two servers:
  - The Authentication Server (AS), and
  - The Ticketing Granting Server (TGS)

GORDON | REYNOLDS (2018)

8

KERBEROS PROCESS: STEP ONE



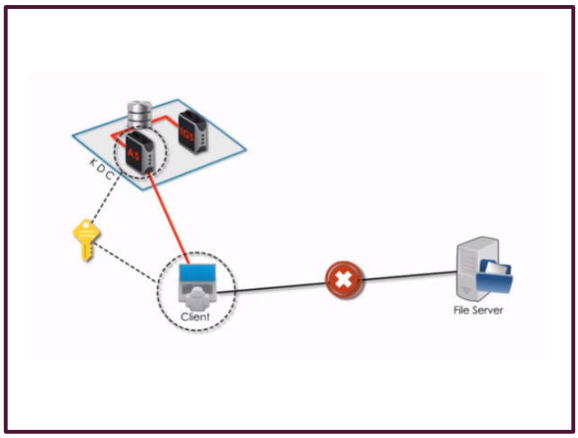
- The Client sends a request to the Authentication Server (AS).
- The request consists of:
  - The user's username, and
  - A request for a ticket to access a server.
- The request is partially encrypted with a secret key
- The secret key used, is the user's password

Note: The user's password is never sent over the unsecure network. It is only used as an encryption key.

GORDON | REYNOLDS (2018)

9

KERBEROS PROCESS: STEP ONE

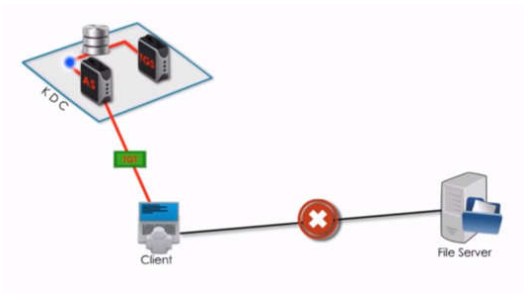


- When the Authentication Server (AS) gets the clients request, it will retrieve their password from the AS database, based on userID.
  - The password is a shared secret key between Authentication Server and Client.
- Their password will then be used to decrypt the user's request.
- If the user's request gets successfully decrypted, the user has been successfully verified.

GORDON | REYNOLDS (2018)

10

KERBEROS PROCESS: STEP ONE

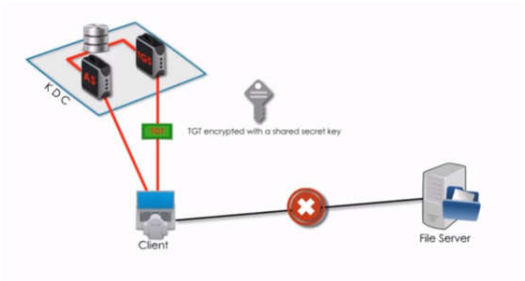


- After verifying the client, the Authentication Server sends back a ticket called a ***Ticket Granting Ticket*** (TGT).
- The TGT is encrypted with another secret key.

GORDON | REYNOLDS (2018)

11

KERBEROS PROCESS: STEP TWO

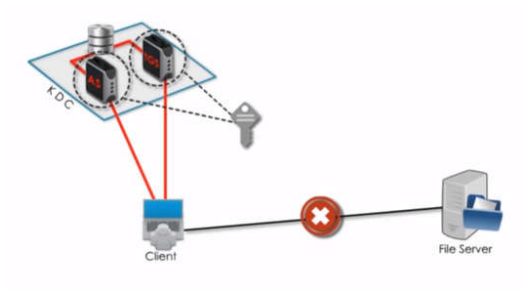


- After the client gets the encrypted TGT, the client sends the ticket to the Ticket Granting Server along with the request for access to the file server.
  - Remember the client can not decrypt the TGT as it does not have the appropriate key.

GORDON | REYNOLDS (2018)

12

KERBEROS PROCESS: STEP TWO

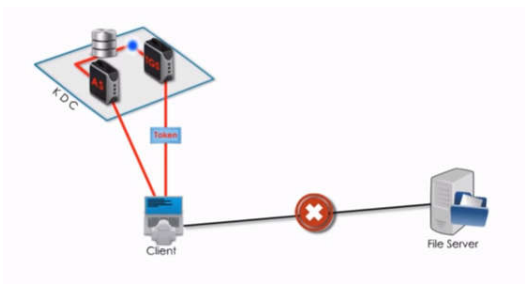


- When the Ticket Granting Server (TGS) receives the Ticket Granting Ticket (TGT), it decrypts the ticket with the secret key shared with the Authentication Server (AS).

GORDON | REYNOLDS (2018)

13

KERBEROS PROCESS: STEP TWO

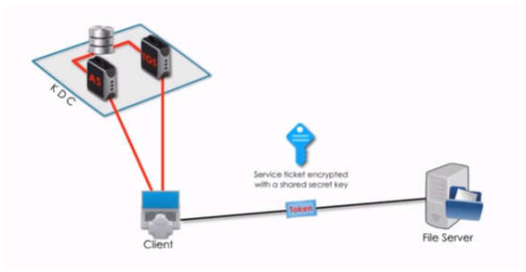


- Then the TGS issues a token that is encrypted with another key.
- This third secret key is shared between the Ticket Granting Server and the File Server (or indeed any other resource that the user is trying to access on the network).

GORDON | REYNOLDS (2018)

14

KERBEROS PROCESS: STEP TWO

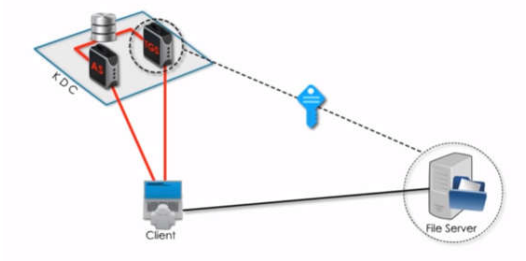


- The Client then sends the token to the file server.

GORDON | REYNOLDS (2018)

15

KERBEROS PROCESS: STEP THREE

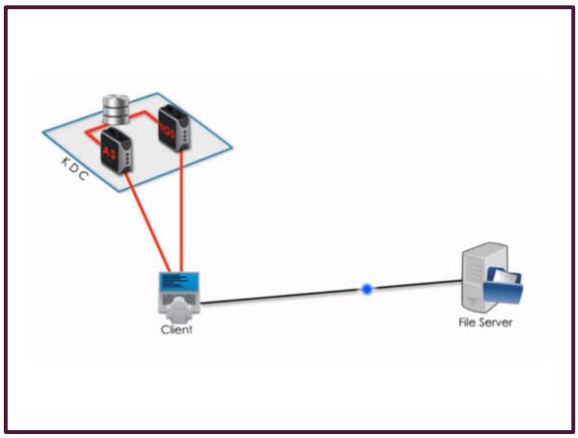


- When the file server gets the token, it decrypts the token with the secret key shared with the Ticket Granting Server.

GORDON | REYNOLDS (2018)

16

KERBEROS PROCESS: STEP THREE



- The file server then allows the Client to use its' resources for a certain period of time according to the token.

GORDON | REYNOLDS (2018)

17

KERBEROS PROCESS: STEP THREE

- The Token is often compared to a movie ticket, it allows you to:
  - Go to the cinema
  - See a certain movie
  - At a certain time
  - On a certain day

GORDON | REYNOLDS (2018)

18

KERBEROS PROCESS: STEP THREE

- All communications between the separate parties require a different key.
- Kerberos is an example of using private key encryption or symmetric key encryption

GORDON | REYNOLDS (2018)

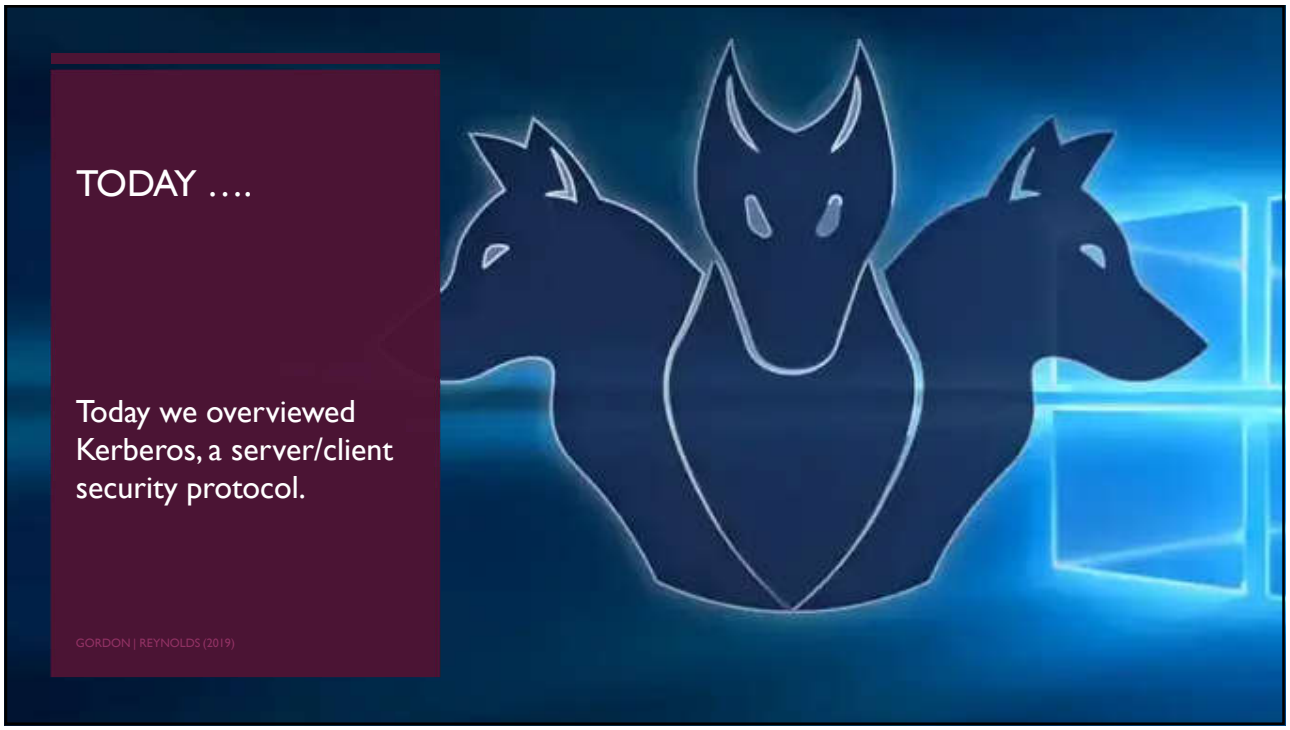
19

KERBEROS: NETWORK TIME SERVER (NTS)

- Kerberos has strict time requirements, which means the clocks of the involved hosts must be synchronized within configured limits.
- The tickets have a time availability period and if the host clock is not synchronized with the Kerberos server clock, the authentication will fail.
- The default configuration per requires that clock times be no more than five minutes apart.
- In practice Network Time Protocol (NTP) daemons are usually used to keep the host clocks synchronized.

GORDON | REYNOLDS (2018)

20


TODAY ….
Today we overviewed Kerberos, a server/client security protocol.
GORDON | REYNOLDS (2019)

21