Computer Security

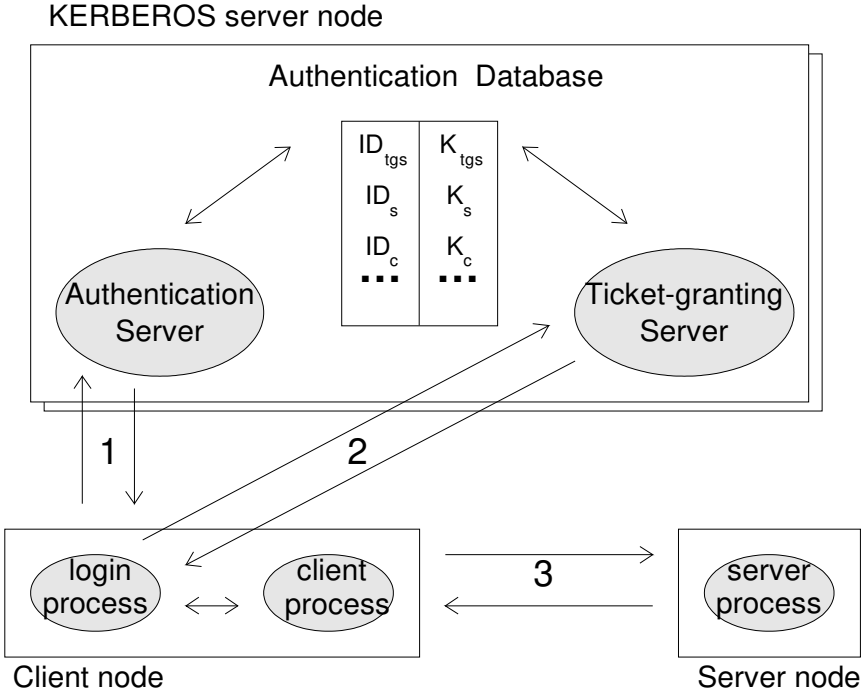
KERBEROS case study
Authentication and Key Distribution

Highlights (v.4)

- developed at MIT and still evolving (last version: 5)
  - http://web.mit.edu/Kerberos/
- used in many places
- Internet standard
- symmetrical system
- user single sign-on

Kerberos' architecture

- Kerberos server
- client processes
- application servers



...Kerberos' architecture (cont.)

Kerberos' server

- executes in a dedicated, physically secure computer
- encompasses:
  - Authentication database
    -> stores secret keys of all system's subjects
  - Authentication server, AS
    -> certifies the users' identities
  - Ticket-granting server[1], TGS
    -> supplies clients with tickets to be used with servers
- it is a KDC, *Key Distribution Center*

1 PT: servidor de bilhetes/emissor de chaves

...Kerberos' architecture (cont.)

Client processes

- execute on “normal” computers
- the user owning client processes is authenticated only once, on log on
- access to services (from application servers) is only possible by means of ticket supplied from Ticket-granting server

Application servers

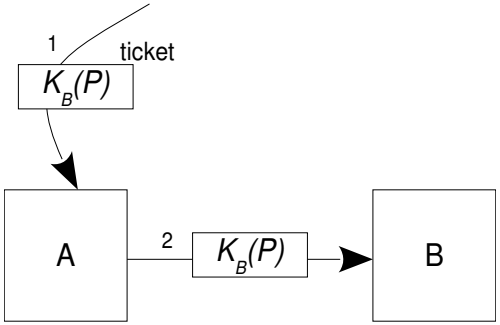
- execute on networked computers
- each shares a specific key with Ticket-granting server
- only serve clients with tickets proved genuine

Authentication (and key distribution) protocol

- based on Needham-Schroeder's authentication protocol
- so, uses the concept of “tickets”

Ticket

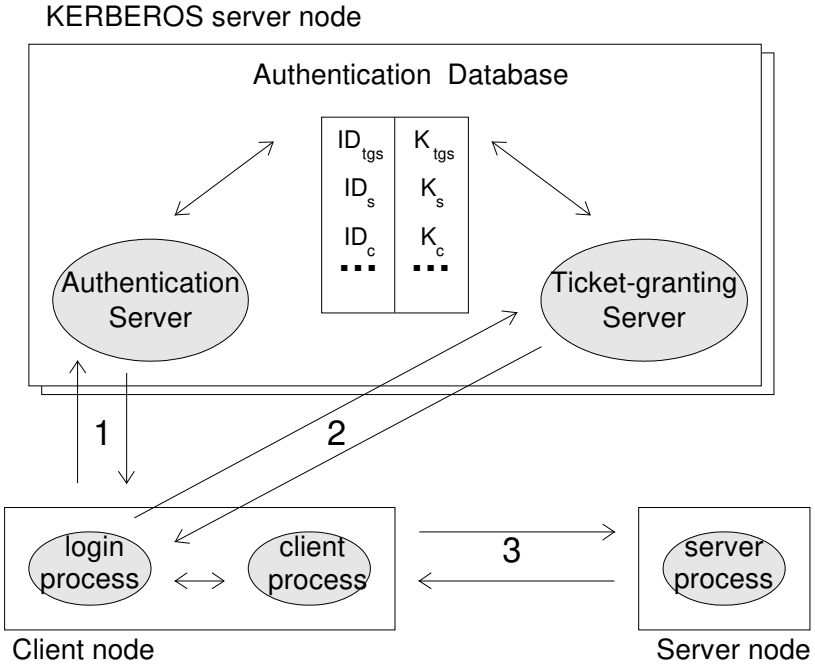
- piece of data delivered to an entity (A) to be forwarded, later on, to another (B)
- the data is ciphered, to be only understood by the final recipient (B)
- typically, contains a session key to be used in conversations between A and B
  - the whole point is to allow A and B to authenticate each other, if they both have already authenticated themselves with the Ticket-granting server!



...Kerberos' authentication protocol (cont.)

Protocol's structure:

1. user's authentication (login) and getting of ticket and key to be used with Ticket-granting server
2. getting of the ticket and key for interaction with an Application server
3. interaction with Application server



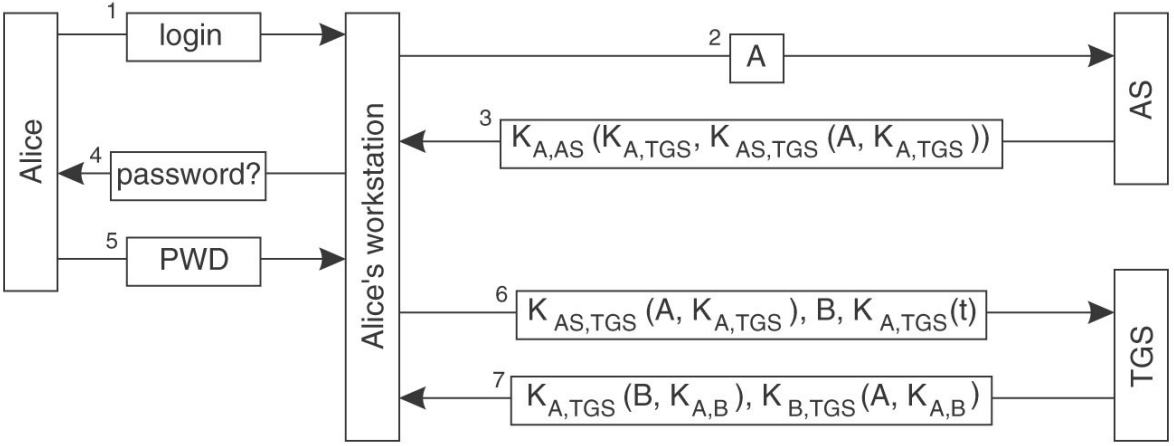


Fig. Kerberos: initial authentication sequence (from *A*), 1-5, and getting of ticket and session key for application server (B), 6-7.

...Protocol's structure: interaction details (cont.)

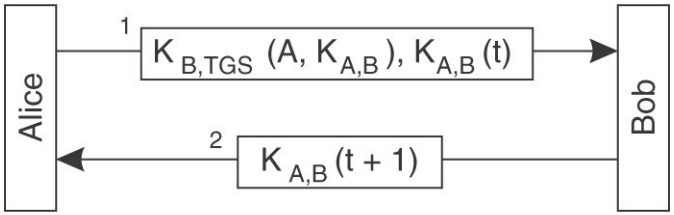


Fig. Kerberos: mutual authentication sequence between Client *A* and server *B*.

Pointers...

- The “**Kerberos system**”, 1988 - S. Miller, B. Neuman, J. Schiller and J. Saltzer
  - ftp://athena-dist.mit.edu/pub/kerberos/doc/techplan.PS
- The “**Needham–Schroeder protocol**”, 1978 - Roger Needham and Michael Schroeder
  - dl.acm.org/citation.cfm?id=359659