Kerberos for Distributed Systems Security

Cunsheng Ding
HKUST, Hong Kong, CHINA

Agenda

- Distributed system security
- Introduction to Kerberos
- Kerberos Version 4 Authentication Protocol
- Operating systems using Kerberos

Distributed Systems Security

Distributed Systems

- A distributed system: a collection of computers linked via some network.

- Characteristic: The components of the distributed system may be under the authority of different organizations, and may be governed by different security policies.
  - Example: The Internet

Security Issues in Distributed Systems (1)

- **Impersonation of user:**
  - A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
- **Impersonation of workstation:**
  - A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.

Security Issues in Distributed Systems (2)

- **Replay attacks:**
  - A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.
- **Conclusion:**
  - In any of these cases, an unauthorized user may be able to gain access to services and data that he or she is not authorized to access.

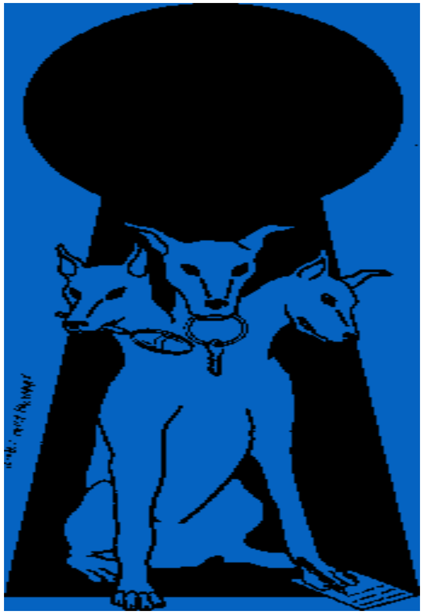
Security Services in Distributed Systems

- Authentication   **********************
- Guarding the boundaries of internal networks
  - Firewalls (covered in this course)
- Access control to distributed objects
  - Access control techniques (not covered)
- Availability
  - Counter DoS techniques (not covered)

Kerberos Version 4
Authentication Protocol

Kerberos Version 4

- Centralized network authentication service
- Developed in the Project Athena in MIT
- In Greek Mythology, the three headed guard dog of Hades



Environment Addressed

- An open distributed environment in which
  - Users at workstations wish to access services on servers distributed throughout the network.
  - Servers can:
    - restrict access to authorized users and
    - authenticate requests for service.
  - Workstations cannot be trusted to identify its users correctly to network services.

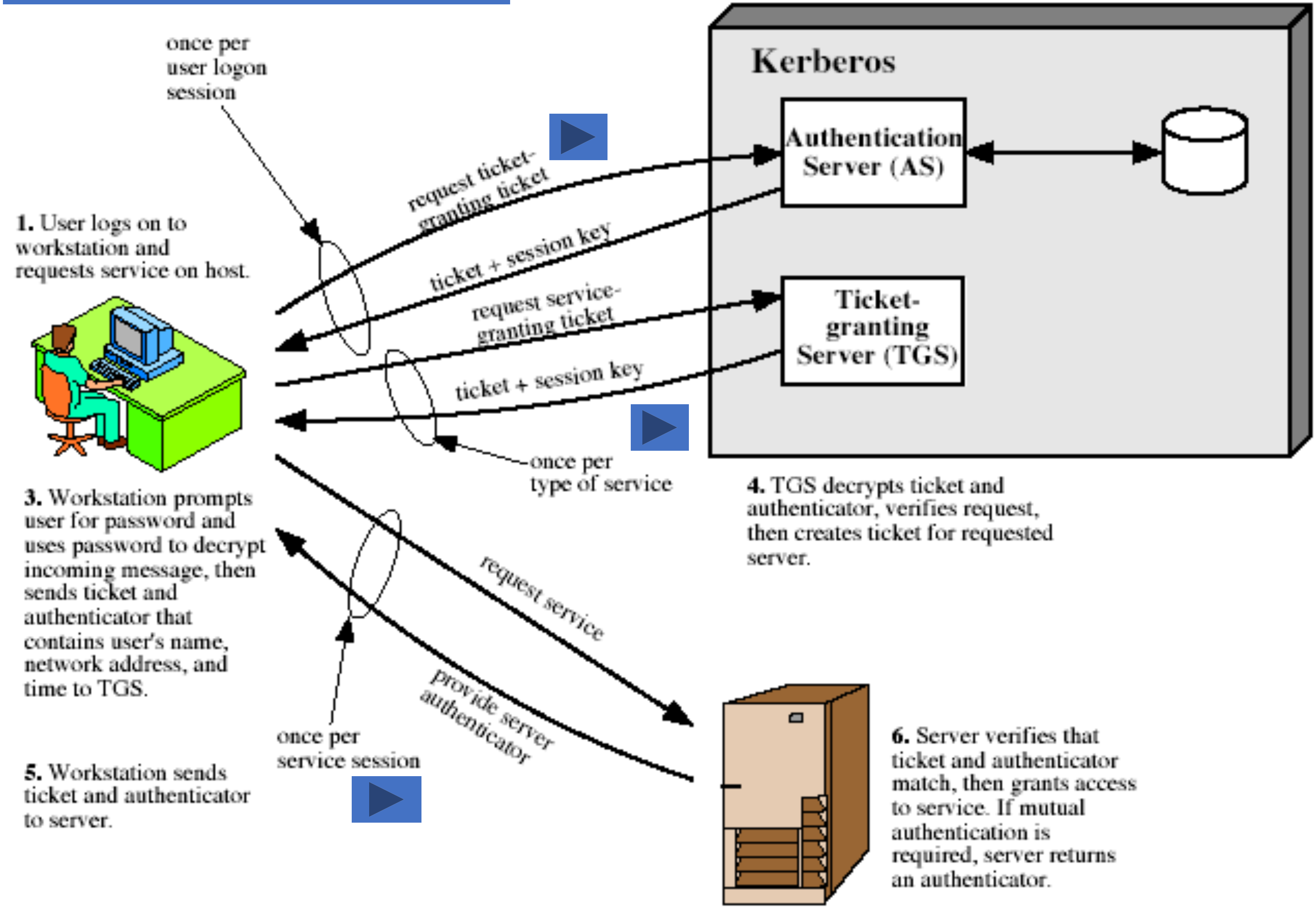
Requirements for Kerberos

- **Secure:** Opponent cannot impersonate a user and the Kerberos service should not be a weak link.
- **Reliable**: Highly reliable Kerberos service to ensure availability of supported services of application servers.
- **Transparent** : Users are only required to enter a password once and don’t know the authentication.
- **Scalable**: System can support large numbers of clients and servers.

Kerberos 4 Overview

- A basic third-party authentication scheme
- Have an Authentication Server (AS)
  - users initially negotiate with AS to identify self
  - AS provides a non-corruptible authentication credential (ticket granting ticket TGT)
- Have a Ticket Granting Server (TGS)
  - users subsequently request access to other services from TGS on basis of users TGT

1. Each user shares a key with AS
2. TGS shares a key with AS
3. All servers are registered with AS


once per
user logon
session
Kerberos
Authentication Server (AS)
request ticket-granting ticket
ticket + session key
request service-granting ticket
Ticket-granting Server (TGS)
ticket + session key
once per
type of service
request service
provide server authenticator
once per
service session

1. User logs on to workstation and requests service on host.

2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.

3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.

4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.

5. Workstation sends ticket and authenticator to server.

6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

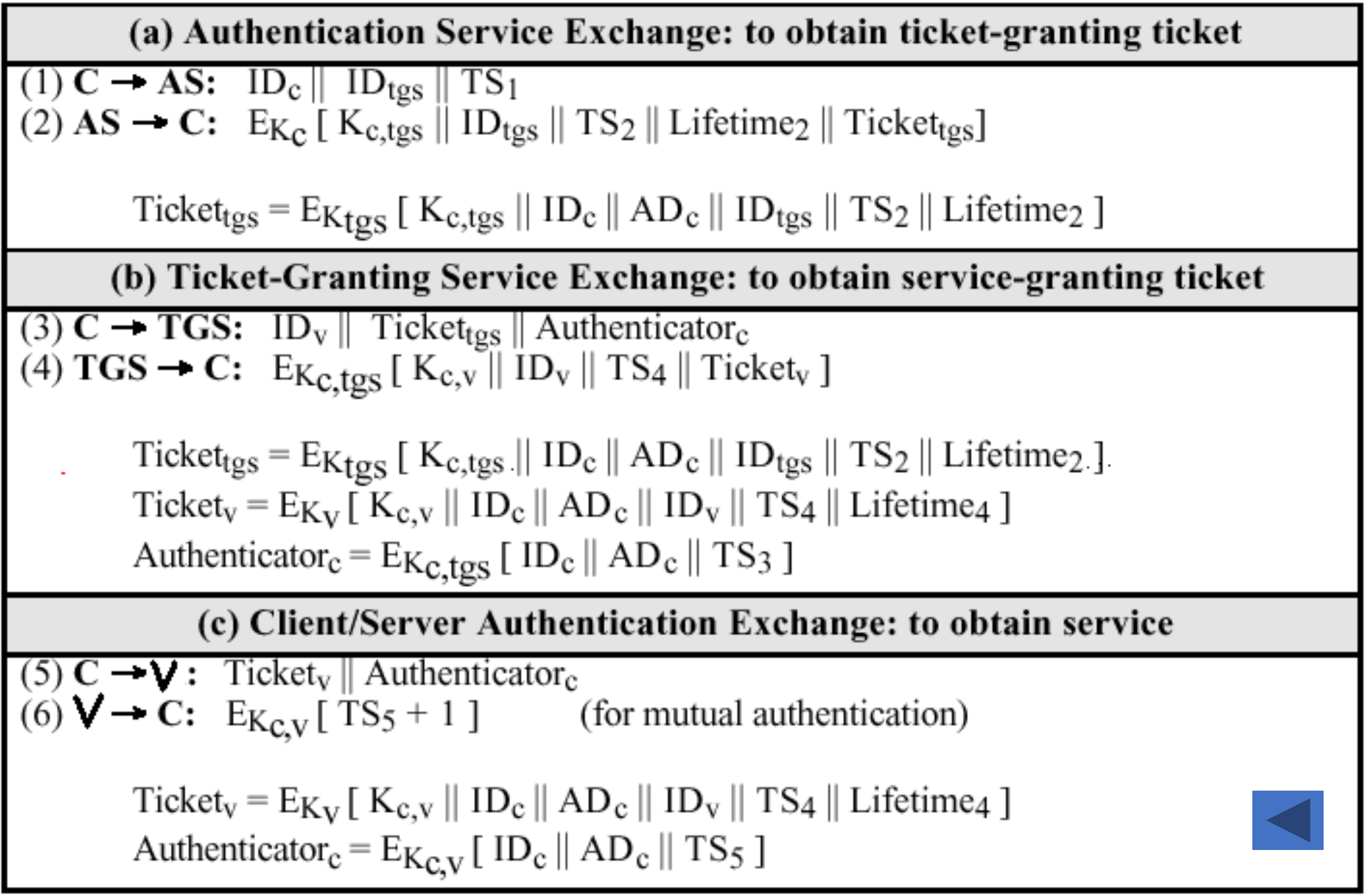
Further Information

- Only one symmetric cipher, i.e., DES, is used in Version 4. In version 5, AES is used.
- Each client needs to share a secret key with the AS only.
- AS and TGS share a secret key for authentication.
- Each server shares a secret key with the TGS.
- ID, timestamp, network address are used for authentication.

Two Ideas in Kerberos

- Protocol 1
  - A → E_k(ID_A|ID_B|timestamp) → B
  - What security services are provided by this protocol?
- Protocol 2: an email ticket for B issued by A
  - A → E_k(ID_A|ID_B|AD_B|ID_V|Period validity) → B
  - V is the email server, AD_B is B's network address
  - K is a secret key shared by A and V
  - It is a ticket for B issued by A. B can use it for email services many times.

Version 4 Authentication Dialogue Overview



(a) Authentication Service Exchange: to obtain ticket-granting ticket

(1) **C → AS:** $ID_c \,\|\, ID_{tgs} \,\|\, TS_1$

(2) **AS → C:** $E_{K_c}[K_{c,tgs} \,\|\, ID_{tgs} \,\|\, TS_2 \,\|\, Lifetime_2 \,\|\, Ticket_{tgs}]$

$Ticket_{tgs} = E_{K_{tgs}}[K_{c,tgs} \,\|\, ID_c \,\|\, AD_c \,\|\, ID_{tgs} \,\|\, TS_2 \,\|\, Lifetime_2]$

(b) Ticket-Granting Service Exchange: to obtain service-granting ticket

(3) **C → TGS:** $ID_v \,\|\, Ticket_{tgs} \,\|\, Authenticator_c$

(4) **TGS → C:** $E_{K_{c,tgs}}[K_{c,v} \,\|\, ID_v \,\|\, TS_4 \,\|\, Ticket_v]$

$Ticket_{tgs} = E_{K_{tgs}}[K_{c,tgs} \,\|\, ID_c \,\|\, AD_c \,\|\, ID_{tgs} \,\|\, TS_2 \,\|\, Lifetime_2]$

$Ticket_v = E_{K_v}[K_{c,v} \,\|\, ID_c \,\|\, AD_c \,\|\, ID_v \,\|\, TS_4 \,\|\, Lifetime_4]$

$Authenticator_c = E_{K_{c,tgs}}[ID_c \,\|\, AD_c \,\|\, TS_3]$

(c) Client/Server Authentication Exchange: to obtain service

(5) **C → V:** $Ticket_v \,\|\, Authenticator_c$

(6) **V → C:** $E_{K_{c,v}}[TS_5 + 1]$ (for mutual authentication)

$Ticket_v = E_{K_v}[K_{c,v} \,\|\, ID_c \,\|\, AD_c \,\|\, ID_v \,\|\, TS_4 \,\|\, Lifetime_4]$

$Authenticator_c = E_{K_{c,v}}[ID_c \,\|\, AD_c \,\|\, TS_5]$

Differences between V4 and V5

Difference Between Version 4 & 5 (1)

- Environmental shortcomings
  - Encryption system dependence
    - Any encryption algorithms can be used in v5 but only DES is possible in v4
  - Internet protocol dependence
    - Only IP is possible → to use any internet protocol

Difference Between Version 4 & 5 (2)

- Environmental shortcomings
  - Ticket Lifetime
    - 1280 minutes (maximum time) → any length of time
  - Authentication Forwarding
    - V4 does not allow credentials issued to one client to be forwarded to some other host and used by some other client. V5 provides this capability.

Difference Between Version 4 & 5 (3)

- Technical deficiencies
  - Double encryption in V4.
  - PCBC encryption (a new mode of operation)
    - In v5, Standard CBC is used

Authentication with Kerberos in Operating Systems

Kerberos in Operating Systems

- It is used in some Windows operating systems
- It is used in the following Unix-like operating systems:
  - FreeBSD, Apple's Mac OS X, Red Hat Enterprise Linux, Oracle's Solaris, IBM's AIX and Z/OS, HP's HP-UX and OpenVMS
- It is used for Kerberos authentication of **users** or **services**.

Comments on Authentication with Kerberos

- Single Sign-On
  - It gives a simple administration.
    - For instance, each user has only one user account within the HKUST domain.
  - It provides good user productivity.
    - For instance, only when each user signs into the HKUST domain, he/she inputs his/her password once, and does not need to retype the password for requesting many services later.