Unit 6: Protection and Security

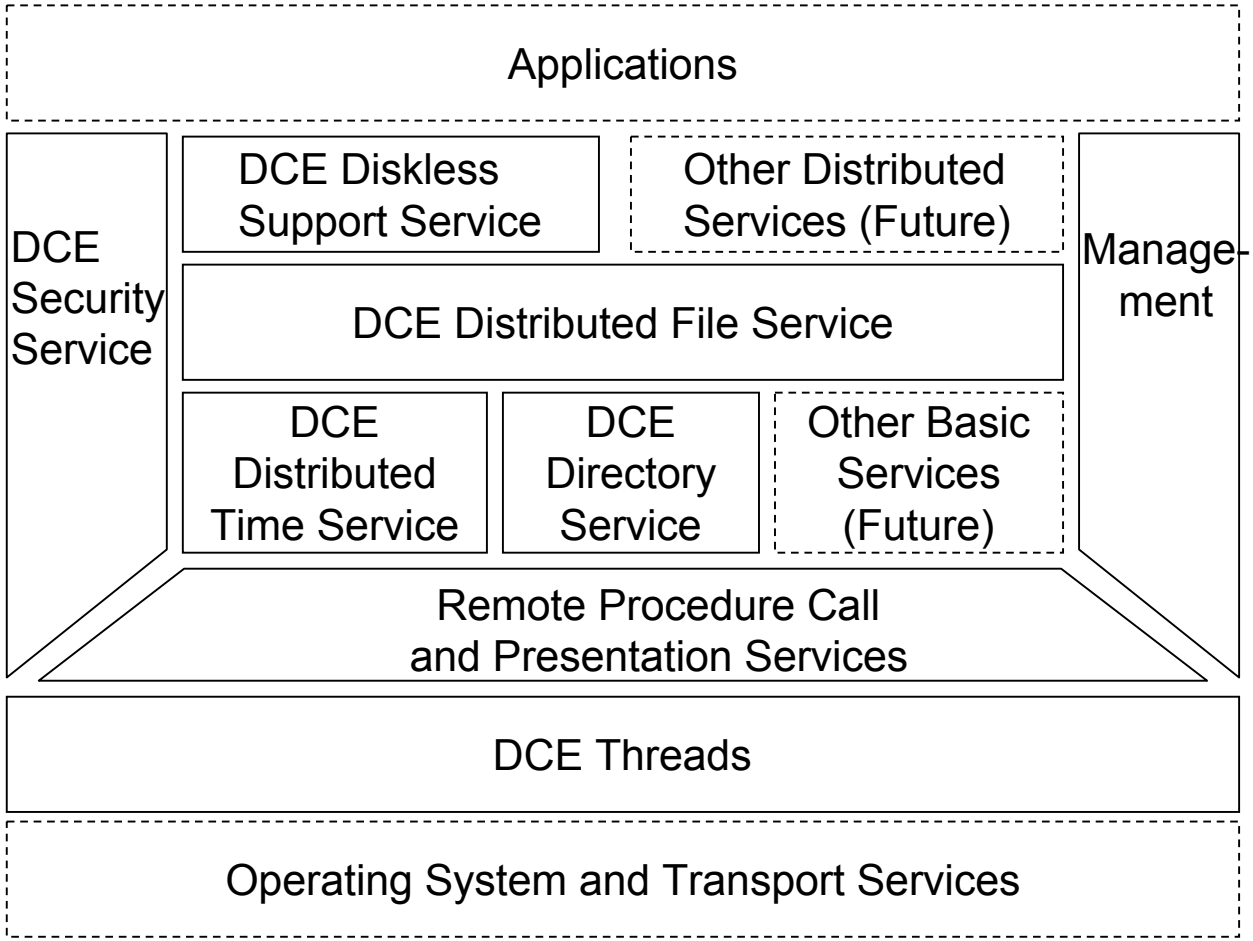
6.7. The OSF Distributed Computing Environment (DCE) and Kerberos

Distributed Computing Environment (OSF™ DCE)

Characteristics of DCE as defined by the Open Software Foundation (OSF):

- Tools for distributed Applications
  - DCE Remote Procedure Call
  - DCE Threads
- Runtime Support for distributed Applications
  - DCE Directory Service
  - Security Service
  - Distributed Time Service
- DCE supports heterogeneous environments
- Client/Server-style Applications
- Communication via RPCs

The DCE Architecture



DCE Threads

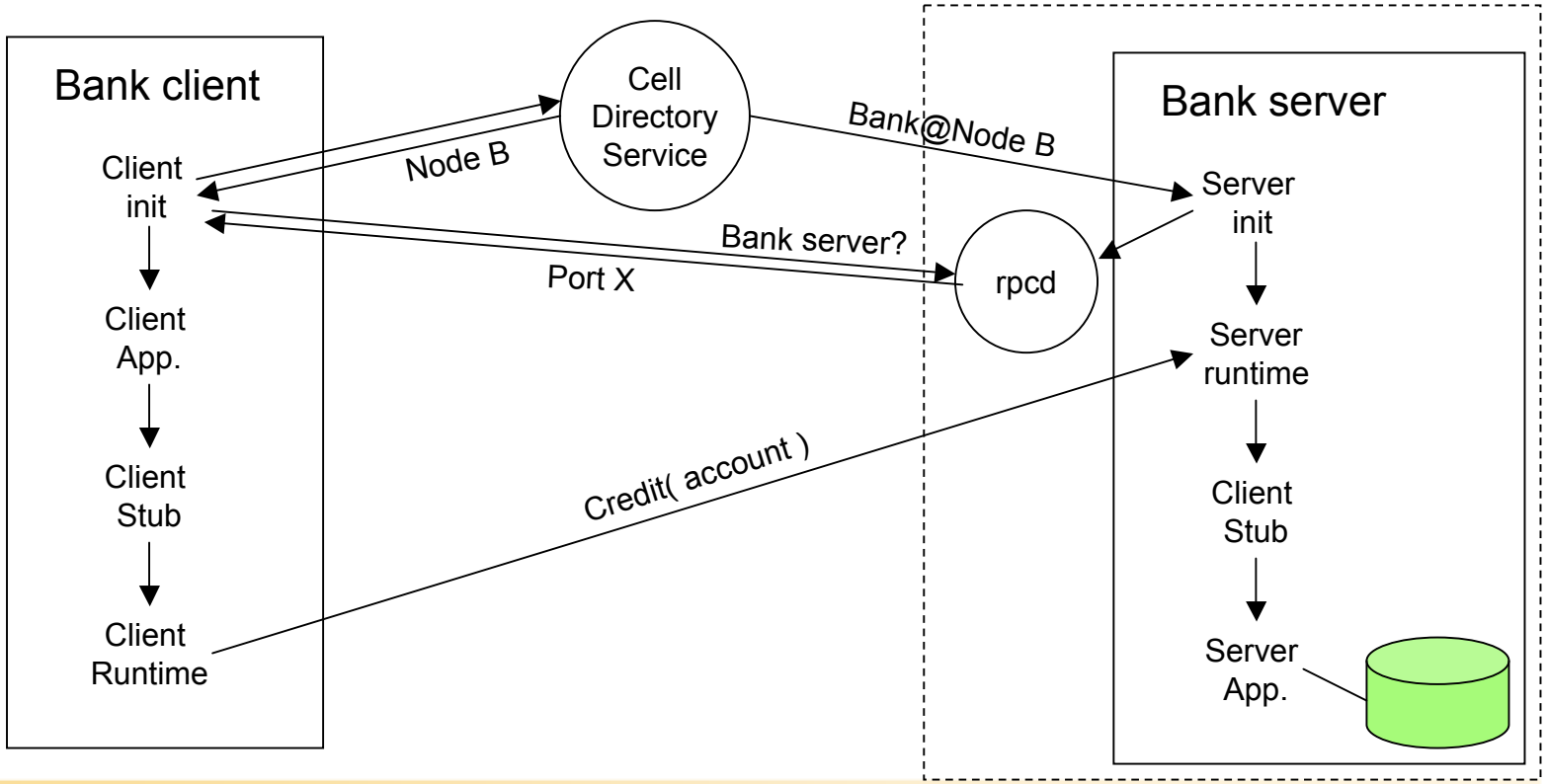
- General characteristics:
  - Based on pthreads (POSIX 1003.4a)
  - Can be mapped onto OS threads
  - Wrapper-routines for non-reentrant system libraries
- Scheduling
  - Priority-based
  - FIFO, Round Robin (RR), RR without priorities (default)
- Communication/Synchronization
  - Mutual exclusion objects
  - Condition variables
  - Join routine

DCE Remote Procedure Call (RPC)

- Client/Server communication, features:
  - Message fragmentation/re-assembly
  - Byte-ordering (network data format)
  - Transparent integration with naming service
  - Based on security service (Kerberos)
- Components of DCE RPC:
  - Interface Definition Language (IDL) with compiler
  - RPC runtime library
  - Authenticated RPC
  - Name Service Independent (NSI) API – interconnection with Cell Directory Service
  - RPC daemon (rpcd), control program (rpccp)
  - Generation of universally unique identifiers via uuidgen

A Distributed Application using DCE

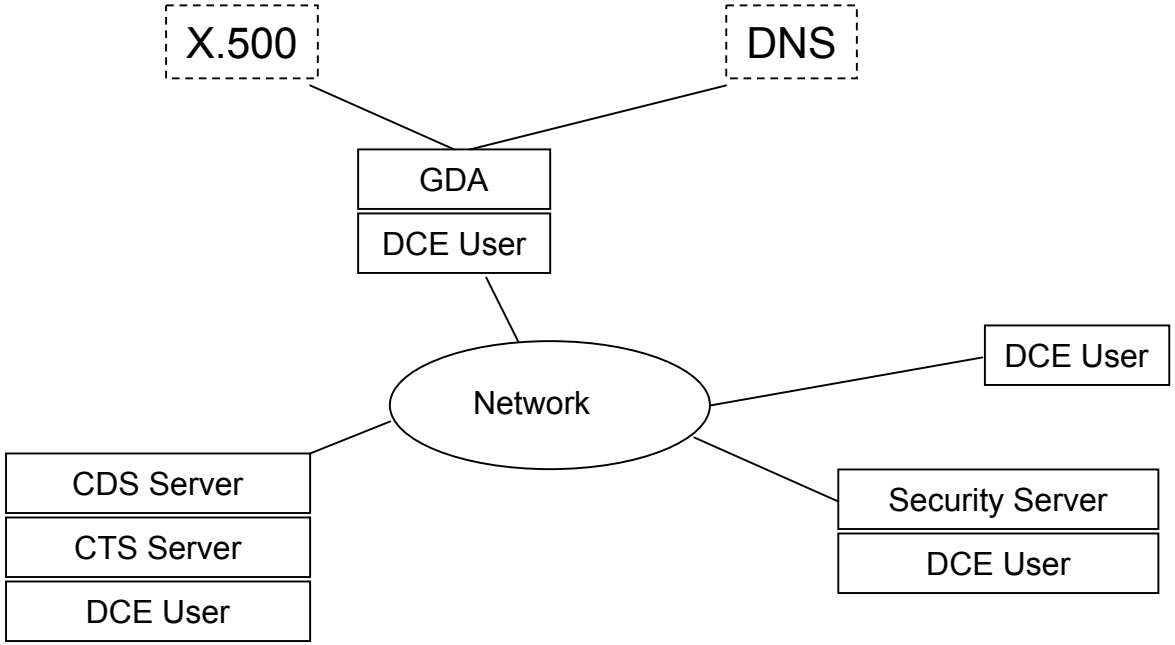
- Binding a client to a server



DCE Directory Service

- Central information repository for distributed system
  - (attribute, value) pairs are stored
- Hierarchical structure
  - Cell Directory Service (CDS)
  - Global Directory Service (GDS)
  - Global Directory Agent (GDA)
  - Directory Service programming interface (API)
- CDS maintains data for a group of machines (cell)
- GDS implements global namespace
- GDA interconnects cells with GDS

Cell connected via GDA



- Cell may access X.500 and Domain Name Service (DNS)
- Cell administrates part of the name space

DCE Security Service

- Three main aspects:
  - Authentication
  - Secure communication
  - Authorization
- Implemented in various DCE components:
  - Authentication service (Kerberos)
  - Registry service (Maintenance of DCE security settings)
  - Privilege service (management of user credentials)
  - Access Control List (ACL) facility
  - Login Facility (initialization of environment)

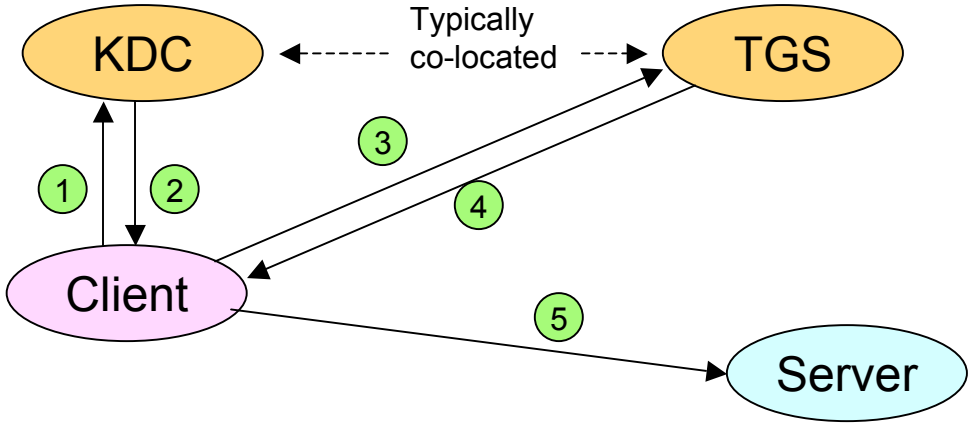
Kerberos Authentication Service

- Developed as part of MIT project Athena
- Kerberos implements an authentication procedure which verifies identity of communication partners
  - DES algorithm, symmetric key encryption
  - Authentication server (Kerberos Server)
  - TGS (Ticket Granting Service)
  - Client proves his identity by presenting an encrypted, service-specific ticket ($T_{c,s}$) when issuing a request
- Kerberos server and Ticket Granting Service (TGS) are assumed to be secure (trusted hosts)

Kerberos principles

- Kerberos requires three main steps:
  1. Client identifies himself against Kerberos Server, he receives a master ticket (the TGT)
  2. Client requests service-specific tickets and prove his identity with the TGT
  3. Client uses service-specific ticket to contact server
- Authentication is transparent from user‘s point of view
  - Modified login program acquired TGT
  - (Client) Applications transparently acquire service-specific tickets
  - TGS-issued tickets and TGT have a default lifetime of eight hours

Kerberos principles (contd.)



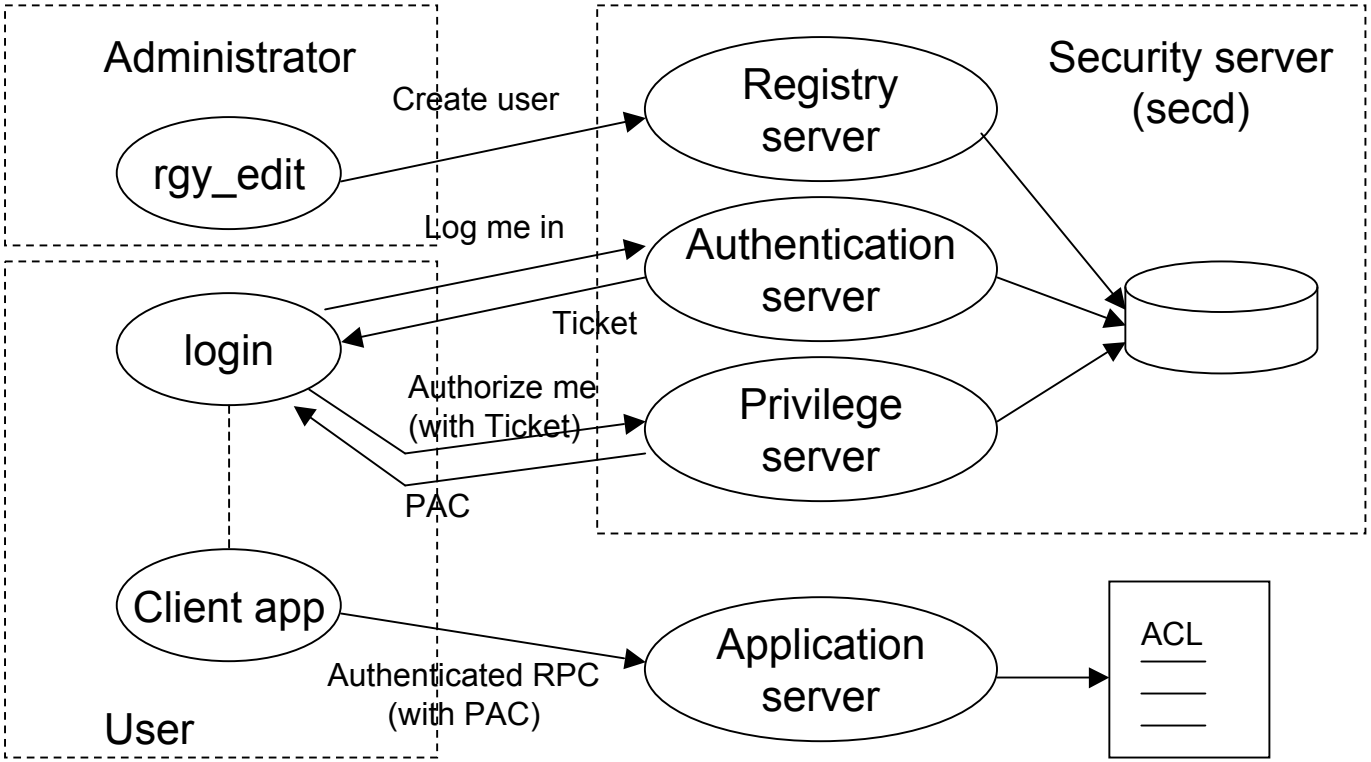
$K_{c:}$ client's secret key
$K_{c,tgs:}$ key for comm. between client and TGS
$\{T_{c,tgs}\}K_{tgs:}$ encrypted ticket for TGS
$K_{c,s:}$ key for client/service communication
$\{T_{c,s}\}K_{s:}$ encrypted ticket for service
$A_{c:}$ authentication info

1. Client -> KDC: c, tgs, n
2. KDC -> Client: $\{K_{c,tgs},n\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. Client -> TGS: $\{A_c\}K_{c,tgs}$, $\{T_{c,tgs}\}K_{tgs}$, s, n
4. TGS -> Client: $\{K_{c,s}, n\}K_{c,tgs}$, $\{T_{c,s}\}K_s$
5. Client-> Server: $\{A_c\}K_{c,s}$, $\{T_{c,s}\}K_s$

Tickets and Authentification info

- Kerberos tickets contain the following data:
  - User name
  - Address of workstation
  - Time stamp
  - Lifetime of the ticket
  - Address of the host running the requested service
  - Session key for client/server communication
- Tickets are encrypted with the server‘s private key (K_s)
- Authentification info (A_c) contains the following data:
  - User name
  - Address of workstation
  - Time stamp
- Authentification infos are encrypted with the session key $K_{c,s}$

Interaction of DCE Security Components



PAC – Privilege Attribute Certificate – Kerberos Ticket with authentication data

Problems with Kerberos

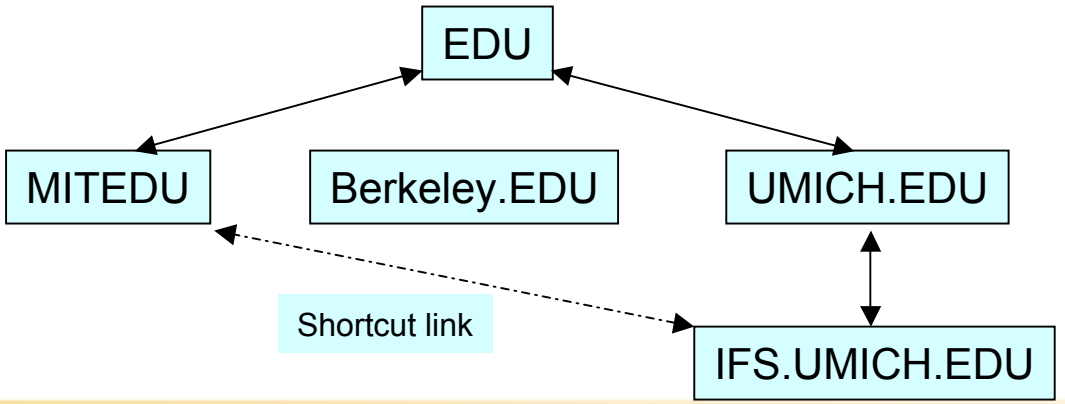
- TGS has to know private keys of all servers
  - Management problem
  - Only communication with well-known system services can be reasonably easy secured
- Server have to remember their DES keys K_s
  - Stored in file system...
- Tickets and authentication info contain time stamps
  - Network-wide clock synchronization required
  - Clock synchronization requires secure comm...
  - Diskless machines are problematic (boot phase)

Kerberos Version 5

- Encryption algorithms in separate software modules
- Keys are typed
  - Can be re-used for different encryption algorithms
- Network addresses may have arbitrary formats
  - Server may specify all supported protocols/addresses in ticket
- Network data format and encryption are standardized
  - ASN.1 format (ISO 8824), no special format for multi-byte data
  - Encryption based on (ISO 8825)
- Tickets contain plaintext section
  - Server may support multiple personalities, actual role is chosen on plaintext info
- Tickets carry starting time and expiration time

Inter-realm support

- Multiple name-spaces communicate in a hierarchy which is based on domain names
  - Inter-real keys allow for interoperability
  - KDC issues tickets for neighbor name spaces in hierarchy
  - Shortcut links are possible
  - Tickets contain path from client to server; server may refuse to act on a ticket whose path contains un-trusted hosts



Kerberos Extensions

- KDC returns special tickets on initial ticket exchange
  - Password can only changed with those special tickets
- Renewable tickets may carry two expiration dates
  - Only valid after first but before second date
- Tickets may be postdated
  - Interesting for batch processing
- Authorization data field
  - KDC copies authorization info from TGT into every newly generated ticket
  - Used by OSF DCE to implement privilege attributed certificates (PACs)
  - Windows 2000 Kerberos supports public/private key for initial authentication (to obtain TGT via user-supplied private key)