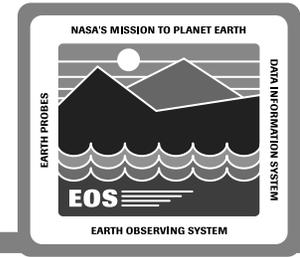


Security In ECS

Manasa Anand

Developers Workshop
30 May 1995

Security in Client/Server Environment



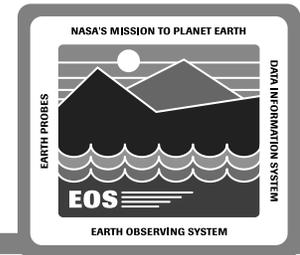
- **Problems**

- Information passing on the wire is not secure (readable and modifiable)
- Verifying the identities
- Restricting service/resource access

- **Major security aspects**

- Data Integrity and Privacy
- Authentication
- Authorization

Data Integrity and Privacy



- **Data Integrity**

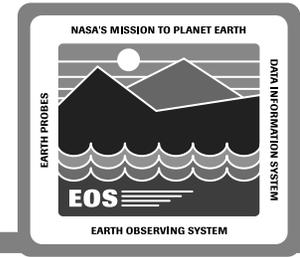
- Ensures that data in transit is not modified
- Achieved through encrypted checksums to the data
 - » Application programmer specifies the protection levels (e.g., *packet_Integrity*)

- **Data Privacy**

- Ensures that data in transit is prevented from eavesdropping
- Achieved through encryption of data
 - » Application programmer specifies the protection level (e.g., *packet_privacy*)

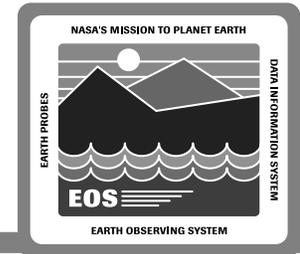
NOTE: Both Integrity and privacy are expensive. Use them sparingly

Authentication



- **Verification of a principal identity without passing the password in clear text**
 - Done through a trusted third party (DCE Security Server)
- **Types of authentication**
 - Principal authentication
 - Client/server authentication

Principal Authentication



- **Interactive principal (user)**
 - Principal gets authenticated during Login
 - Password supplied on the command line, but is not passed on the wire
- **Non-Interactive principal (server)**
 - When a host is booted, a server need to acquire a different identity than the default (root)
 - How ?
 - » Password maintained in a local keytabfile
 - » Servers acquire identities using the keytabfile
 - » KeyTabFile created through “rgy_edit” utility

NOTE: Application Programmer must have this file protected.