Seguridad
en Ambientes Grid

Prof. Jesus De Oliveira
Prof. Yudith Cardinale

Agenda

- Introducción al Seguridad en ambientes grid
- Requerimientos de seguridad
- Modelo de seguridad GSI
- Certificados proxys

Introducción a la seguridad Grid

- **En un entorno grid,**
  - Instituciones ceden recursos de cómputo y almacenamiento
  - Usuarios emplean recursos de cómputo y almacenamiento de forma distribuida

- **Los usuarios y recursos se agrupan en organizaciones virtuales (grupos con intereses de trabajo colaborativo)**

- **Dado el dinamismo y envergadura de una plataforma grid, la gestión de la seguridad presenta el problema de garantizar mecanismos de seguridad desde un punto de vista distribuido**

Introducción a la seguridad Grid

- **¿Por qué es importante la seguridad?**
  - Como institución que cede recursos:
    - ¿Los usuarios que utilizan mis recursos son auténticos y estàn autorizados?
    - ¿Pueden estos usuarios ejecutar acciones maliciosas que degraden mis servicios y los datos de mis usuarios?
    - Existen mecanismos confiables que permitan auditar las acciones de los usuarios que acceden a mis recursos?
  - Como usuario que utiliza recursos
    - ¿Los datos que estoy colocando en un recurso pueden corromperse o manipularse por usuarios no autorizados?
    - ¿Las comunicaciones entre mi estación de trabajo y el Grid pueden ser interceptadas y manipuladas por terceros no autorizados?
    - ¿Puede garantizarse que mi identidad no puede ser usurpada para realizar acciones maliciosas o en detrimento de los servicios y otros usuarios?

Requerimientos de seguridad

- **Autenticación**
  - Identificación confiable entre componentes del grid
  - Identificación confiable de usuarios ante componentes del grid
- **Autorización**
  - ¿Qué actividades se les permite realizar a los usuarios identificados?
  - Pertenencia de usuarios a organizaciones virtuales
- **No-repudio**
  - Garantizar la auditabilidad de las operaciones que realizan los usuarios
- **Integridad y confidencialidad**
  - Garantizar que las comunicaciones y datos no sean interceptadas o alteradas por terceros

Modelo de seguridad GSI

- **GSI: Globus Security Infraestructure**
  - Basado en tecnologia de certificados digitales X.509 y claves públicas y privadas
  - Cada usuario se identifica con un *certificado digital*: un archivo con sus datos personales y clave pública
  - Los certificados de usuarios son *avalados* por *entidades certificadoras (CA)*, que aseguran que la identidad del usuario es real y válida. Este aval es provisto por la *firma electronica* del certificado por la CA
  - Se establecen relaciones de confianza entre autoridades certificadoras, de manera que los recursos del grid *confian* en la información contenida en un certificado *firmado* por alguna CA en la que se confía

Modelo de seguridad GSI

- **GSI: Globus Security Infraestructure**
  - Los recursos del grid (componentes) también se identifican entre si usando certificados digitales firmados por autoridades certificadoras con relaciones de confianza mutua
  - La comunicación entre cualquier componente del grid es *asegurada* con encriptamiento del canal de comunicación, usando el protocolo de comunicación segura SSL (se usan las claves privadas de los mismos certificados)
  - Ciertos componentes proveen información de membresía de usuarios a organizaciones virtuales (operando de forma distribuida)
  - En cada componente se definen *reglas* de acceso en base a la membresía de usuarios a organizaciones virtuales

Certificados proxys

- **En un ambiente grid puede ser necesario que un componente pueda identificarse ante otro *como si fuera el usuario que originalmente solicitó el servicio***
- **Certificados Proxy:**
  - Certificado temporal (dura máximo 12 horas) que identifica al usuario original
  - En lugar de poseer una firma digital de la CA, posee una firma digital del certificado original del usuario (se establece una *cadena de confianza o jerarquía de firmas digitales*)
  - Poseen restricciones sobre cuáles operaciones pueden realizarse por servicios o usuarios identificados con ellos
  - Si es "robado" sólo permitiría al atacante identificarse como el usuario auténtico únicamente ante el servicio autorizado, y hasta que expire la validez corta del proxy

Preguntas