Security[1]

Typical grid scenario

- Large number of resources, pooled together
- Large user pool
- Resources may be owned and operated by different groups
- Problem: Restrict access to the resources, yet allow for collaboration

Grid security requirements

- Users want to be able to communicate securely
- Fundamental concepts
  - Privacy
    - The only users who can understand conversations must be invited
    - Use encryption in all communications
  - Integrity
    - Message should not be changed during transmission
    - Use signed messages
  - Authentication
    - Verify that the entities are who they claim to be
    - Use certificates
  - Authorization
    - Allow or deny access to services based on policies
- Requirements
  - Identity
  - Authentication
  - Message protection
  - Authorization
  - Single sign on

Identity and authentication

- Each entity should have an identity
- Entity: User, service, or system
- Authenticate
  - Establish identity; is the entity who he claims he is?
  - Established by driver's license, username/password
- As ecure communication should ensure that the parties involved in the communication are who they claim to be

[1] Most of the material in this set of notes is from the Educational division of Open Science Grid.

- Stops masquerading imposters
  - We should be protected from malicious users who try to impersonate one of the parties in a secure conversation
- Solution can be based on use certificates

Message protection: Privacy

- Real life applications may contain sensitive data
  - An application on cancer research may contain scientific proprietary data
- Need to ensure privacy for information sent over the grid
  - Information on medical record; patient number 3456
  - Information sent over the grid should be known only to sender and receiver; no one should be able to listen in on the message
  - Solved with encryption mechanisms
- Secure conversation should be private
  - An eavesdropper should not be able to make sense out of it

Message protection: Integrity

- Make sure that no one is tampering with the message
  - A malicious person should not be able to replace `whoami` with `rm -f *`
- A secure communication should ensure the integrity of the message
  - The receiving end must be able to know for sure that the message received is exactly the same as sent by transmitting entity
- Generally achieved by signed messages

Authorization

- Establishing rights
  - Processes need to use resources but which resources are allowed
  - Does a certain user have access to certain service or resource?
- What can a said entity do?
  - Are you allowed to be on this flight?
    - As passenger?
    - As pilot?
  - Unix `rwx` permissions
- Must authenticate first

Grid security: Single sign on

- Grid jobs are long running jobs
- Should you authenticate every single time your job needs to access a resource or service? Not feasible
- Single sign on is a mechanism to simplify this case
  - You authenticate once with the grid, and your jobs will run on your behalf
  - Delegate your rights for the use of services; these services will act on behalf of the user, with user's rights
- Important for complex applications that need to use grid resources
  - Enables easy coordination of various resources
  - Enables automation of process
  - Allows remote processes and resources to act on user's behalf
  - Authentication and delegation

Revisit typical grid scenario

- Need to provide access to shared services – cross-domain authentication, authorization, accounting, billing
- Support multi-user collaboration
  - Organized in one or more *Virtual Organizations*
  - May contain individuals acting alone – their home organization administration need not necessarily know about all activities
- Leave resource owner always in control

Issues

- Resources may be valuable and the problem being solved sensitive
  - Both users and resource providers need to be careful
- Resources and users are often located in distinct administrative zones
  - Cannot assume cross-organizational trust agreements
  - Different mechanisms and credentials
- Dynamic formation and management of communities (VOs)
  - Large, dynamic, unpredictable, self-managed
- Interactions are not just client/server, but service-to-service on behalf of the user
  - Requires delegation of rights by user to service
- Policy from sites, VO, users need to be combined
  - Varying formats
- Want to hide as much as possible from applications

Cryptography for message protection

- Solution for privacy using encrypted messages

- Enciphering and deciphering of messages in secret code
- Key
  - Collection of bits
  - Building block of cryptography
  - More bits, the stronger the key
    - 256 bits key is stronger than 128 bits
    - The longer the key, the longer it takes to decrypt
  - Most algorithms are well-established and tools have been already developed for performing the computations
- Encryption
  - Data treated as a stream of bits
  - Process of taking some data and a key, and feeding it into a function to get encrypted data out
  - Encrypted data is unreadable unless decrypted
- Decryption
  - Process of taking encrypted data and a key, and feeding it into a function to get back the original data
  - Encryption and decryption functions must be linked
- Asymmetric encryption
  - Encryption and decryption functions using a *key pair*
  - Keys are mathematically linked
- Public and private keys
  - With asymmetric encryption, each user can be assigned a key pair: a private key and a public key
  - Private key is known only to the user
  - Public key is given away to the world
  - Encrypt with public key, decrypt with only private key
  - Message privacy
    - Message encrypted with public key will only be decrypted with private key
    - Guarantees the integrity of message

Digital signatures

- Used to ensure message integrity
- Allow the world to
  - Determine if the data has been tampered with during transit
  - Make sure no masquerading takes place
  - Verify who created a chunk of data
- Sign with private key, verify with public key
- Signatures are generated and sent with the message

Public Key Infrastructure (PKI)

- An arrangement that binds public keys with respective user identities by means of a certificate authority (CA)
  - Allows you to know that a given public key belongs to a given user
- User identity must be unique for each CA
- Binding is established through registration and issuance process
- Builds off of asymmetric encryption
  - Each entity has two keys: public and private
  - Private key is known only to the entity
- For each user, the user identity, the public key, their binding, validity conditions, and other attributes are made unforgeable in public key certificates, issued by the CA
  - Public key given to the world encapsulated in an X.509 certificate
- PKI arrangements enable computer users to be authenticated to each other, and to use the public key certificates to encrypt messages to each other
  - PKI consists of client software, server software, hardware, legal contracts and assurances, and operational procedures
  - A signer's public key certificate may be used by a third party to verify the digital signature of a message, made using the signer's private key
  - PKI enables the parties in a dialog to establish confidentiality, message integrity, and user authentication without having to exchange any secret information in advance
- Certificate authorities
  - An authority that exists only to sign user certificates
    - An example of a trusted third party
    - Characteristic of many PKI schemes
  - Issues digital certificates which contain a public key and the identity of the owner
    - Attests that the public key contained in the certificate belongs to the person, organization, server, or other entity noted in the certificate
    - CA's obligation is to verify an applicant's credentials so that users and relying parties can trust the information in the CA's certificates
  - CA signs its own certificate which is distributed in a trusted manner
  - Verify CA certificate, then verify issued certificate
  - If CA is subverted, the security of the entire system is lost