Security and Virtual Organisation Management in XtreemOS

* Sécurité informatque : prévention et detection d’actions non authorisées par des utilisateurs d’un système informatique :
* Keep the bad guy out
* Let him in, but keep him from doing damage
* Be sure about the identity of the user
* …
* Grid Security is security to enable Virtual Organisationss
  + Security in a Grid OS :
    - Native support for VO management
    - Leverage OS security support to protect resources
    - Transparent security management
    - Scalability in security
* Virtual organization :
  + a temporary or permanent coalition of geographically dispersed and autonomous participants including individual and/or organisations, who agree to share resources in the system in order to fulfill their tasks
  + VOs are used as a bridge to provide a Grid security solution based on trust
  + Establishing trust :
    - Personal recommendations
    - Reputation from trusted sources
    - Cryptographic verification
* An entity uses computer programs to cryptographically verify the information given
  + If everything is ok, then trust of the information is established
  + Otherwise, there is not trust
* Public key encryption
  + Users possess public/private key pairs
  + Anyone can encrypt with the public key, only one
  + person can decrypt with the private key
* Certification Authorities :
  + The CAs are responsible for certifying the public keys of different users who subscribe to the CA
  + CAs are entities that are trusted by different systems
  + An end entity is
    - Person, role (“Director of marketing”), organisation, pseudonym, a piece of hardware or software, an account (bank or credit card)
  + CA manages key lifecycle: creation, store, delete, renew
* Open Grid Services Architecture (OGSA) Security :
  + Secure functionality should be cast as services
  + Leverage on existing and emerging WS security standards
    - Authentication service;
    - Identity mapping service
    - Authorisation service; etc.
* GSI – Grid Security Infrastructure :
  + A reference specification for Grid security architectures
  + Protocols and APIs to address Grid security needs
  + Based on public-key encryption technology
  + Each user as a Grid id, a private key, and a certificate signed by a CA
  + First implementation – in the Globus Toolkit
* Authentication in GSI
  + Certificate-based authentication (PKI)
  + GSI certificate includes information such as
    - Subject name;
    - public key belonging to the subject;
    - Identity of the CA; and
    - Digital signature of the named CA
  + Certificates are obtained via established protocols
* Single Sign On and Delegation
  + Jobs require access to multiple resources
  + Need to automate access to other resources: Authenticate Once
    - Allows remote processes and resources to act on user’s behalf – also known as delegation
  + Solution adopted in the GSI: proxy certificates
    - A temporary key pair in a temporary certificate signed by your ‘long term’ private key valid for a limited time (default: 12 hours), but can be renewed
* XtreemOS System :
  + A XtreemOS system consists of
    - A set of resource machines from one or more participants
    - A set of Grid-wide system services
    - A set of VOs to support cross-machine resource sharing and logical isolation of resource usage within the system
  + A user of a XtreemOS system is defined as another system
* Building Up Trust in XtreemOS
  + XVOMS Certificate
  + User registration with XVOMS
  + RCA (Root certification authority) registration with XVOMS
  + Machine registration with RCA
* Advantages of XtreemOS Trust Model
  + User management is separated from resources management
  + Scalability in resource management
  + SSO and Delegation not depending on proxy certificates
* Conclusion :
  + Scalable VO management
    - Independent user and resource management
    - Interoperability with VO management frameworks and security models
    - Customizable isolation, access control and auditing
  + Very Dynamic VOs
    - Short-lived VOs created automatically for the duration of an application/workflow
      * Multi-users
    - Lightweight configuration of resources
    - Predefined policies (VO-based)
  + Improving usability
    - Local resource administrator: autonomous management of local resources
    - VO administrator: flexibility management of credential and VO policies
    - End user: login as a Grid user into a VO; the Grid should be as much as possible invisible
  + Secure and reliable application execution
    - Fine-grained control of resource usage
* On-going and Future Work
  + Traceability
    - Exploiting tokens for traceability in SSO
  + Security monitoring and auditing
    - Rule-based monitoring systems; including aggregation of events and logs for auditing purpose
  + Interoperability by using third-party identity providers
    - Shibboleth; myProxy
  + Evaluating how to adapt some services for the Cloud
    - Identity as a service