Privilege Management Infrastructure / Authorization Architecture

Terminology

Four phases of design and specification:
- Codifying privilege and policy
- Designing a delegation model
- Establishing trust anchors and acquiring privilege
- Defining operational procedures

Phase One: Codifying Privilege and Policy

- Need to be able to write down (in a machine readable / machine processable manner) the privilege that a subject has, and what a verifier will require in order to render a decision
- Codifying privilege is the simpler task.
- Many different choices for syntax:
  - Proprietary
  - BNF
  - ASN.1
  - SAML
• Codifying policy is a more complicated task

• One interesting standardization effort is XACML
  o Requirements for a policy language
  o Rule, Policy, PolicySet
(see also a recent variation, JACPoL)

• Why is codifying policy harder than codifying privileges?

• Protection and communication of both privilege and policy

Phase Two: Delegation Model

• Need a (precisely-controlled) way to pass on privilege

• Universal constraint

• Sub-delegation

• Two types of delegation (based on the semantics of the action performed):
  o Does the delegation assign privilege, or
  o Does the delegation confer authority to act on behalf of the delegator?
• Two methods to assign privilege

• Practical considerations in delegation (research topics)
  o Delegating “down”
  o UI for delegation
  o Temporal validity