Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

A Persona-Based Framework for Flexible Delegation and Least Privilege

Coimbatore Chandersekaran
William R Simpson
Andrew Trice

19 October 2007

Agenda

- Need for delegation in IT systems
  - Extra challenges in military/IC enterprises
- Proposed delegation framework
  - Persona concept
  - Scenarios
  - Registration service
- Support for least privilege
  - Need for least privilege
  - Scenarios
  - Registration service
- Delegation invocation process
- Summary
  - Advantages
  - Status in Air Force context

Need for a Formal Delegation Process

- Continuity of operations
  - Acting for a boss/commander in their absence/incapacity
- Efficiency
  - Boss has official authority, but not the time or expertise
- Managing transitions
  - Overlapping roles for limited period during turnover

Need for a Formal Delegation Process – Con't.

- Least privilege
  - "delegating to a role"--getting user to act in correct capacity
- Delegation is bounded in time
  - Specific time period
  - Good until canceled / expired / delegate leaves / event completed
- Need to provide accountability and attribution for delegated activity.

Delegation -- Challenges in military enterprises

- Security clearance level restrictions
- Need for rapid deployment – the “chop”
- Legal restrictions / accountability
- Delegation across multiple security domains
- Persona definitions based on AF Enterprise IA architecture
  - All active entities are credentialed using PKI
  - Access Control by groups and roles (GBAC)
  - Illustrations assume Active Directory (not necessary to concept)

The Persona concept

- A persona is a special category of user that embodies only delegated privileges
  - **Advantage**: The persona appears as a “real” user and all mechanisms put in place for the user work, including identity, authorization and access, and federation.
    - Persona may be assumed only after “real” human user taking on persona explicitly chooses it, or may be mandated by current context (DEFCON, THREATCON, Trust Agreements, etc.)
    - The delegate persona is the responsible party for actions and attribution (delegator is still accountable)
    - The delegation must be recorded and registered in advance through a delegation registration service, and the delegation must be approved by written policy
    - Necessary data and mechanics must be implemented to support persona and provide traceability

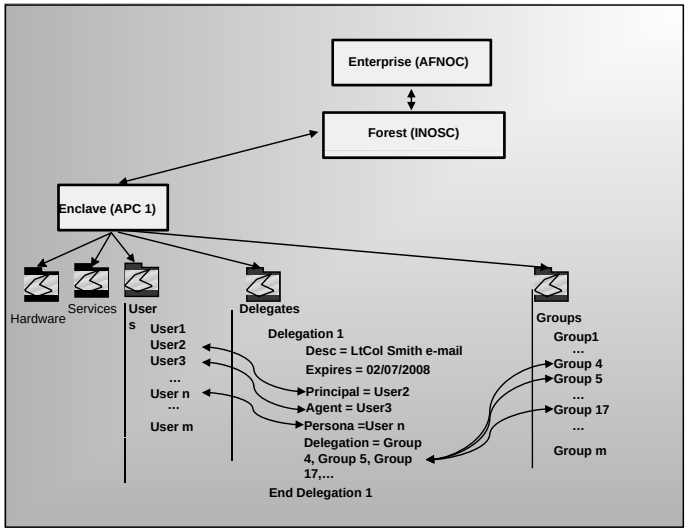
The Persona concept– data and mechanics

- The existence of a persona delegation in the user file:
  - The logon script may include a call to the delegation service for possible revision of identification of the user.
  - Logon may include automatic delegation when external conditions require it.
- The system opens a session with:
  - Original credentials assigned to the individual
  - Or delegation credentials that are provided by the persona.
- The delegate persona is:
  - Persistent (in our illustration), although it should have an expiration date at the end of which it is renewed or expires (“persona non grata”).
  - May be transient in uses for coalition, temporary aliances, and other temporary events (dynamic delegation) – not dealt with at this time.
- Audit records:
  - Verbose during delegation process
  - Attributed to persona and session number.

The Persona concept– data and mechanics (Con’t)

- The delegate persona can be retrieved as a delegate by query to the delegation data base.
- When a related persona is created, the attributes under the user are modified.
- The last entry is provided with “Delegate”, as an indication for delegation services. This field may have a default of “Normal”, and a created Persona may have a value “Persona”.
- Principal-agent delegation can be used to implement personas

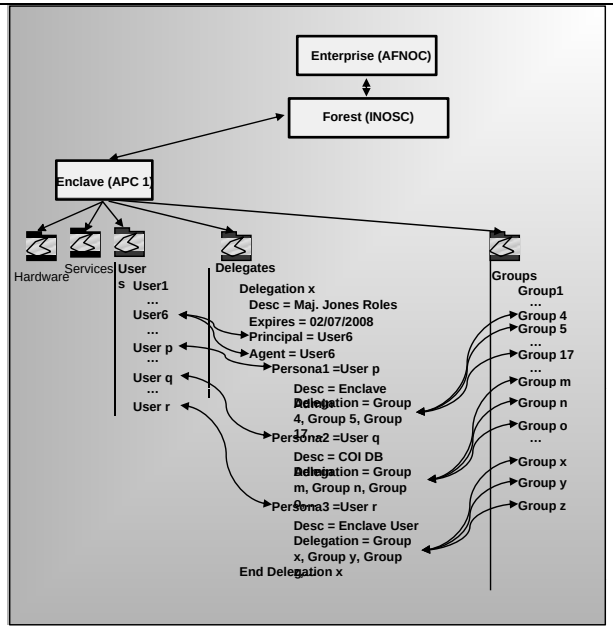
Principal – Agent Delegation Architecture -- Registration



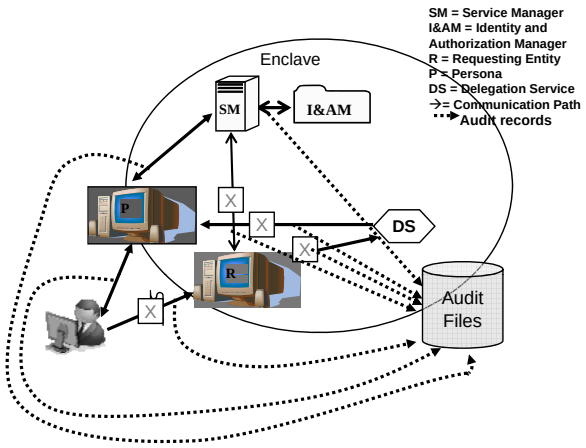
Least privilege

- Concept: A user must be able to access only such information and resources that are necessary to its legitimate purpose.
- Principle is an important design consideration in enhancing the protection of data and functionality from faults and malicious behavior.
- Need often arises out of the need to manage the extent of activity that can take place, or the cost of errors by the human operator.
  - User requests a catastrophic action and acknowledges the request without mulling over the consequences (formatting a hard drive, for one).
  - Under these circumstances the user will be left to establish the least privilege to accomplish the task.
- Principal-Principal delegation can be used to implement least privilege

Principal – Principal Delegation Architecture -- Registration



Delegation Invocation Process



Additional Uses of Personae

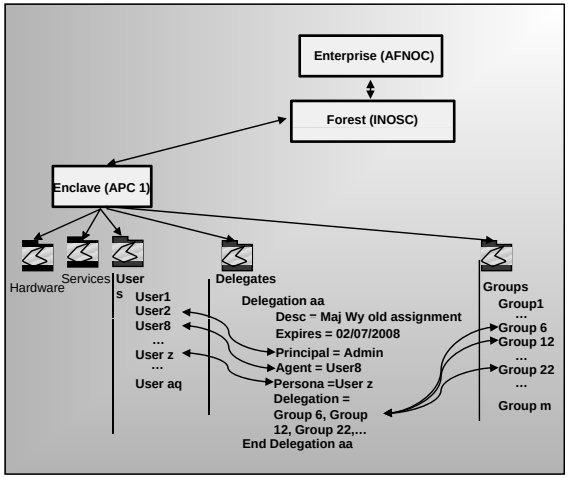
- Impossible to foresee all uses at this time, but two are being actively explored:
  - Use of multiple personae during period of job overlaps (transfers or “Chops”)
  - Use of personae for attribution of virtual machines. The personae would need to be created at the time of virtual machine implementation.

Summary

- Advantages
  - Flexibility and Usability
  - Tracking and accountability
  - Modest additional infrastructure needed
- Status in Air Force context
  - Is under consideration for incorporation as part of infrastructure build out

Backups

Admin-Principal Delegation – “the chop”



Delegation use cases

Function	User Role	Interface Notes
Invoke Registration authority	Invoke Service	User Identity Details and authorities
Identify Delegation Agent Principal-Agent Delegation	Any Potential Authorized User	Must be able to read delegation policy, and access DIT. Must screen delegation pair and limit choices.
Identify Delegation Agent Principal-Principle Delegation	Administrator	Must be able to read delegation policy, and access DIT. Must screen delegation pair and limit choices.
Identify Delegation Agent Admin-Agent Delegation	Administrator	Must be able to read delegation policy, and access DIT. Must screen delegation pair and limit choices.
Identify delegation attributes	Any Potential Authorized User	Probably a choice of attributes are presented that meet policy. Otherwise choices must be screened.
Release of Delegation	User identified as principal in one or more delegations	Presentation of choices for delegate deletion. Persona is removed from registry. Expiration is also a release of delegation.

Delegation use cases (cont.)

Function	User Role	Interface Notes
Invoke Delegation	Login script invokes Service	User Identity Details and authorities. Present delegations for the user that have been registered
Chose delegation for session	Any Potential Authorized User	Must be able to read delegation policy, and access DIT. Must redirect user to persona and break all links with prior user.
End Delegation	Any Persona	Terminate session only.

Delegation services

Service	Level for Service	Other Services Needed
Set up Delegation Service	Admin	Provide rules and linkages to delegation services, update rules as policy changes.
Create Delegation	Any Potential Authorized User	User Identity Details and authorities. Present delegations for the user that have been registered
Delete Delegation	Any Principal for Principal-Agent delegations, others require admin authority	Must be able to read delegation policy, and access DIT. Must be able to eliminate persona.
Invoke Delegation	Any Potential user flagged in login script	Must be able to read delegation policy, and access DIT. Must redirect user to persona and break all links with prior user.