SECURITY ARCHITECTURE

In this section, we will approach grid service security with a detailed discussion on the security challenges faced by the grid community in general, and then explore the details of security solutions provided by the OGSA. Resource sharing among heterogeneous virtual organization participants is a complex process because of the challenges faced in integration, interoperability, and trust relationship.

We can further explain this by examining the following factors:

Integration Challenge. There are numerous security frameworks, comprehensive standards, and implementation available today. The majority of these organizations, individuals, and/or resources have their own preferences about the security requirements that are most suitable for their own environment. We cannot replace all these security frameworks, nor are we able to come up with a common alternative. This places the burden on the participants to honor the existing security frameworks and/or seamlessly integrate with them. This, in turn, requires that the OGSA security architecture be "implementation agnostic," so that it can be instantiated in terms of the existing security mechanisms; that is, "extensible" so that it can incorporate new security services when available; and capable of integration with the existing security services.

Interoperability Challenge. The resource sharing of these interoperable resources may extend into many domains of security realms, and their respective needs security interoperability at each layer of service implementation. Let us examine these various levels in the following points:

- At protocol level, different domains need to exchange messages across their protocol layers and they need to have interoperability at each layer of the protocol stack.
- At the policy level, secure interoperability requires each party to specify any policy it may wish to enact in order to enter into a secure conversation, and these policies need to be interoperable and mutually comprehensible.
- At identity level, we require mechanisms for identifying a user from one domain to another domain. For any cross-domain invocation to succeed in a secure environment, the mapping of identities and credentials to the target domain identity is absolutely required.

Trust Relationship Challenge. The trust among the participants in a dynamic virtual organization is the most complex thing to achieve, and this trust must be evaluated for each session or request. This requires federation of a trust relationship among the participants.

To summarize, for the security challenges in a grid environment, one must ensure the following points are addressed while categorizing the solution areas:

- Integration solutions where interfaces should be abstracted to provide an extensible architecture.
- Interoperable solutions, to enable services to invoke each other even when they are hosted by different virtual organizations with different security mechanisms and policy requirements.
- Define, manage, and enforce trust policies within a dynamic grid environment.

emphasizes the security challenges we have discussed earlier in this discussion, and their solution dependency. As indicated by the relationship arrows, a solution within a given category will often depend on another category.

.Figure 7.8. The categories of security challenges are complex in a grid environment