Security Model

Historically, E2E's security model was driven by the objective of establishing a proper separation of concerns between security staff and application engineers. E2E wanted to offer a strong, yet simple framework where security policies are transparently applied to all services. Security staff were meant to be able to perform consistent improvements over time, independently of any application or service development.

At the same time, the security model was not supposed to negatively impact the creativity and flexibility required by application developers. Especially now that organizations begin to iteratively reshape their service landscape as part of evolving SOA and EDA initiatives, frequent changes to applications and services are the norm and must be possible without affecting cost, time and risk.

Taking note of the fact that every organization concerned with security will want to reuse previous infrastructure investments, E2E's security model was designed to leverage and augment existing capabilities, rather than forcing organizations to adopt an intrusive, product specific model that E2E would impose.

Direct model execution proves to be a perfect basis for dealing with security issues. By modeling security policies in UML, and then executing them as designed, the risk of divergence between design intent and practical implementation is entirely eliminated. In contrast to code, models can be reviewed much more easily, making security audits effective – and fast. Simultaneously, best practices are more consistently enforced.