Real Life Use of CORBA Security and RAD

A Case Study in the Product Development Environment

Jeff Cahoon
Director Server Engineering
iWitness Inc.
jeff.cahoon@iwitness.com

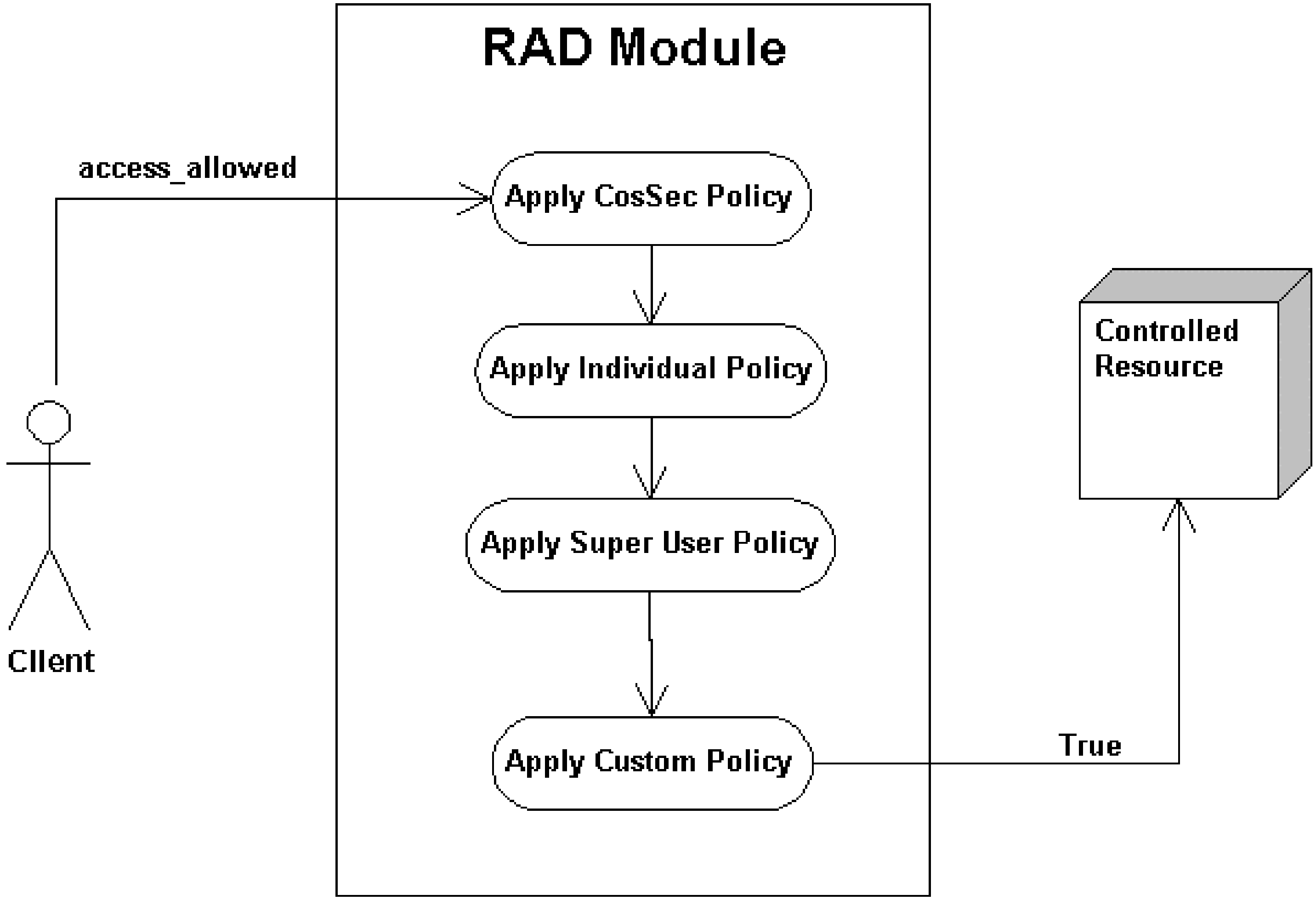
Problem Space

- Records Management
  - Security, chain of custody, carefully controlled deletion, significantly different data types.
- Regulatory Compliance
  - Catch all relevant metadata and content, allow searching and sharing, adaptability to changing laws (International), business and technology.
- Capacity Management
  - Seamless integration with popular tools (economic retrieval).

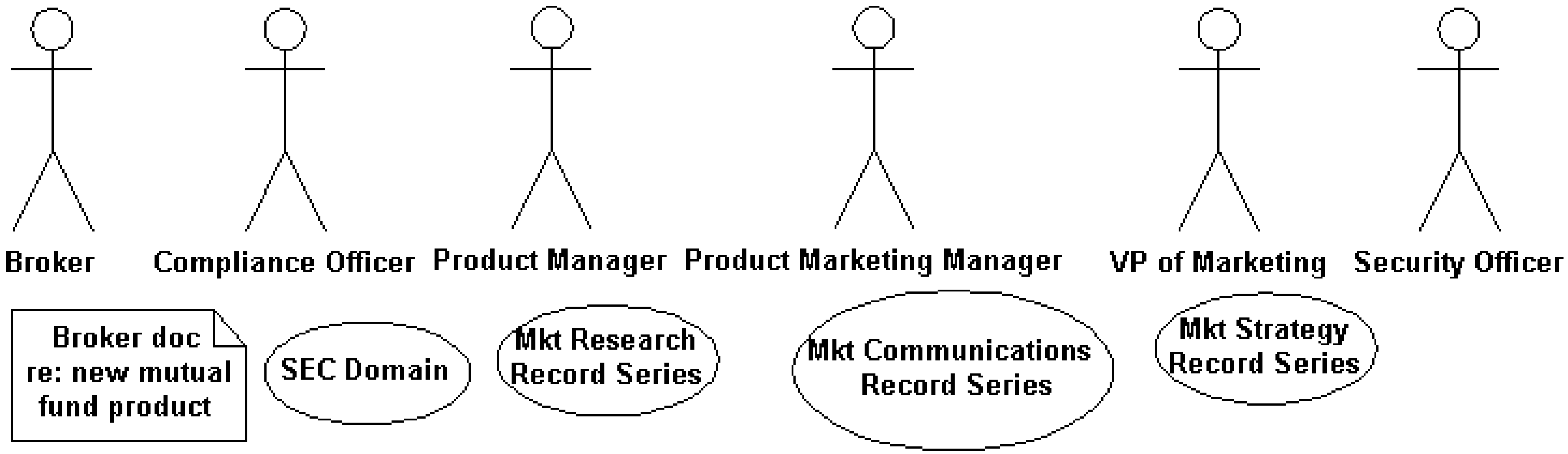
Difficulties to Overcome

- Target access control for extremely sensitive data.
- Many changing groups of users in various roles.
- Vast numbers of records and users with few administrators.
- Different security requirements in orthogonal domains for various portions of the same record or different record operations.
- The need for accurate accounting of accesses or attempted accesses along with convincing proof that security was not bypassed (chain of custody).

Picture of Security Infrastructure



Security Model for a Document


Broker
Compliance Officer
Product Manager
Product Marketing Manager
VP of Marketing
Security Officer
Broker doc re: new mutual fund product
SEC Domain
Mkt Research Record Series
Mkt Communications Record Series
Mkt Strategy Record Series

The same record could be a member in many record series or domains and may be accessed through several RAD policies.

Access Paths

- The Broker sees the record through the RAD Individual Policy.
- The record is also exposed through the CosSec policy. The Compliance Officer sees the SEC domain, the Product Manager sees Mkt Research, the Product Marketing Manager sees Mkt Communications, VP Marketing sees Mkt Strategy.
- The Security Officer sees the record through the RAD Super User Policy.

Our CosSec Experience

- What it did for us – scalable and flexible general structure for regulatory compliance.
- What was hard – GUI presentation for business users, defining domains and groups, multiple domains spec problem, gsum flags.
- How we implemented it – without orb integration, hidden as a policy inside of RAD, commercial CosSec products could not handle flexible domain assignment for resources.

Our RAD experience

- What it did for us – data level security, overriding policies (blacklists, super users), allows libraries of policies for selection and combination through GUI.
- What was hard – cannot use to “gray out” menu options, cannot handle partial access.
- How we implemented it – called access_allowed before resource access, no orb interceptors, requires application programmer understanding.

Expected Extensions in Future

- GUI for policy aggregation
- Dynamic Policy Definition
- Uses for hierarchical groups
- Users for hierarchical domains
- Delegation and Roles
- Non-repudiation
- Auditing
- 3rd Party CosSec module