Attribute based Access Control Model for Multi-Mission Data in Space Ground System

GENERAL DYNAMICS
Mission Systems

Somdatta Nath
somdatta.Nath@gd-ms.com

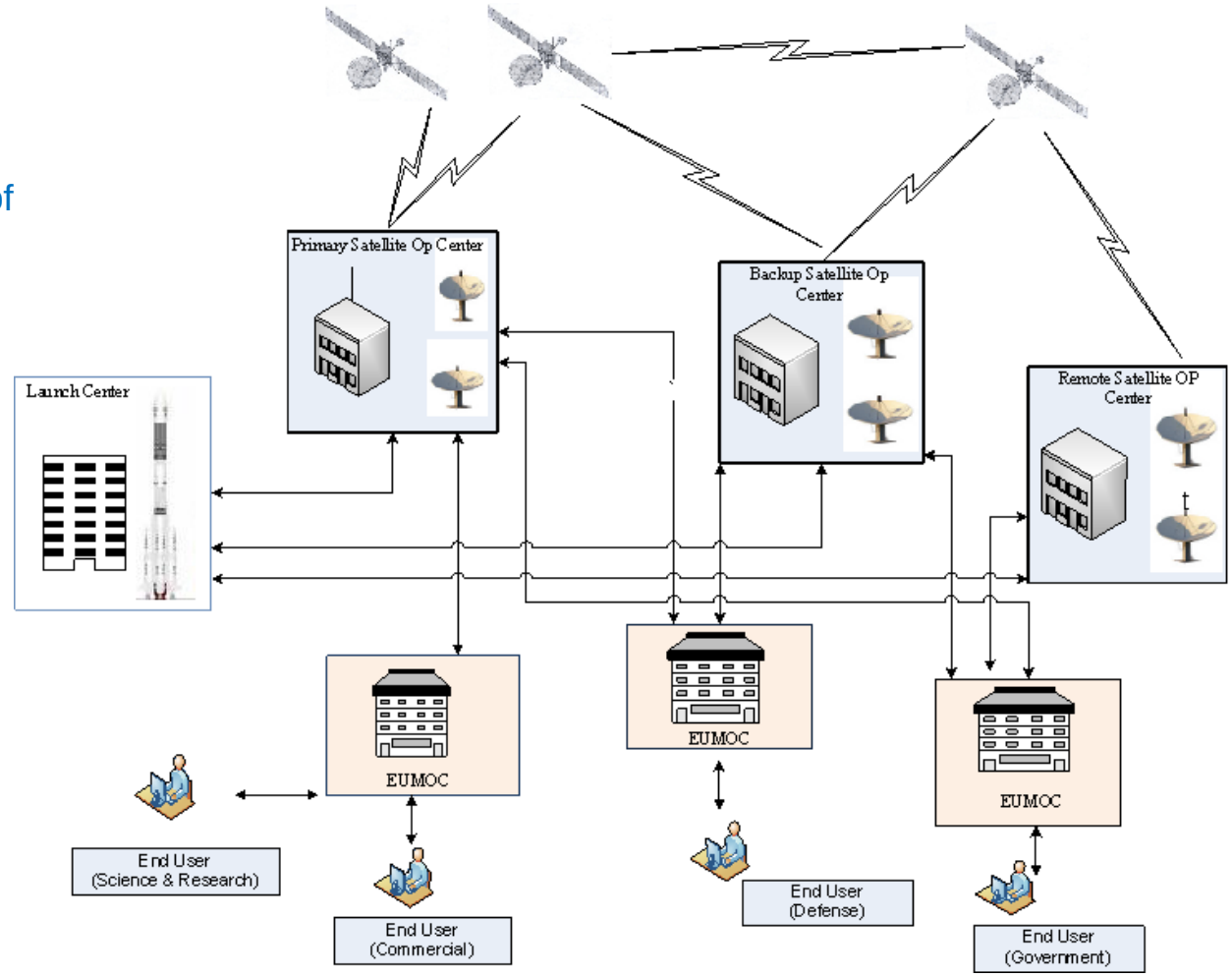
Overview of Discussion Topics

- Functional architecture of a typical Space Ground System with multiple external users.
- Data Access Control requirements of a classical Multi-Mission Space Ground System.
- Highlights of existing schemes for Access Control : strengths and weaknesses of these schemes with respect to Multi-Mission Space Ground System.
- Limitation of existing schemes for defining Multi-Mission Space Ground System Data Access.
- Key points of present scheme, Attribute based Access Control Model for Multi-Mission Data in Space Ground System, ABAC-MG.
- Implementation highlights of ABAC-MG scheme for a model Multi-Mission Space Ground System.
- Performance of the ABAC-MG scheme.
- Summary.

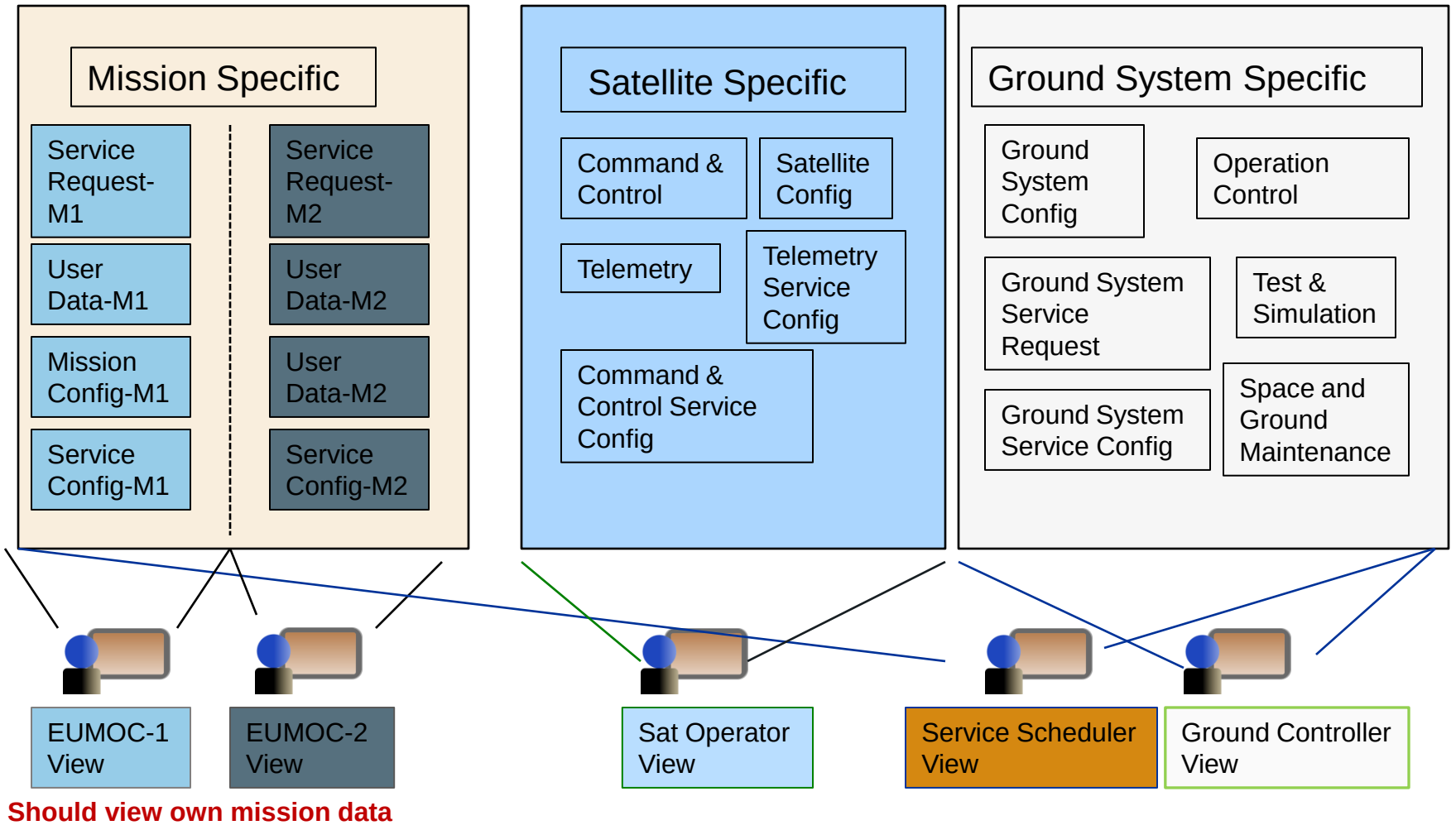
Structure of a Typical Space Ground System

Key Elements :

- Space (segment) includes Satellite Fleet.
- Launch (segment) consists of equipments and services for Launch.
- Ground (segment) responsible for maintaining communication between space segment and end users.
- User (segment) requests and uses satellite services.



Space Ground System Data View



In order to secure Space Ground System Data, "minimum privilege" principle needs to be applied to control access to data.

Ground System Data Access Requirements

- A specific EUMOC should access only its Mission Data.
- Different Mission Operation Centers control different missions, some are for scientific research, commercial purpose like weather monitoring, some are for Classified missions.
- It is not desirable to provide indiscriminate access to MOC data.
- A specific EUMOC may need to specify different access level for its personnel
- It is very likely for a MOC to control multiple missions.
- A MOC may need to define access permission to mission/s data. Some personnel may need access for one mission while some may need access permission for multiple/all mission data.
- A MOC may also define different access permission for different data objects for the same mission.

Ground System Data Access Requirements (contd.)

- EUMOCs may access certain Ground System Data.
- In order to submit service request, EUMOC may need to access service specific Ground System data defined and specified by service architecture.
- EUMOCs may not be given access permission for other Ground System Data objects, including ground system specific service configuration data, satellite configuration data etc.
- Ground System personnel need to access data to perform necessary operation.
- Satellite Operator may need to see only Satellite specific data
- Scheduler may need permission to access all Mission and Ground System data in order to schedule services.

Access Control is essential in Space Ground System to protect data from un-authorized access as well as to permit MOC and Ground System personnel to carry out required operations.

Existing Methods of Data Access Control

At the Application Layer:

•Developing customized queries to return authorized set of data

•Using Application frame work security and declarative techniques

Pro :

•Security is uniquely suited for the application need.

•Fine Grained access can be defined.

Con:

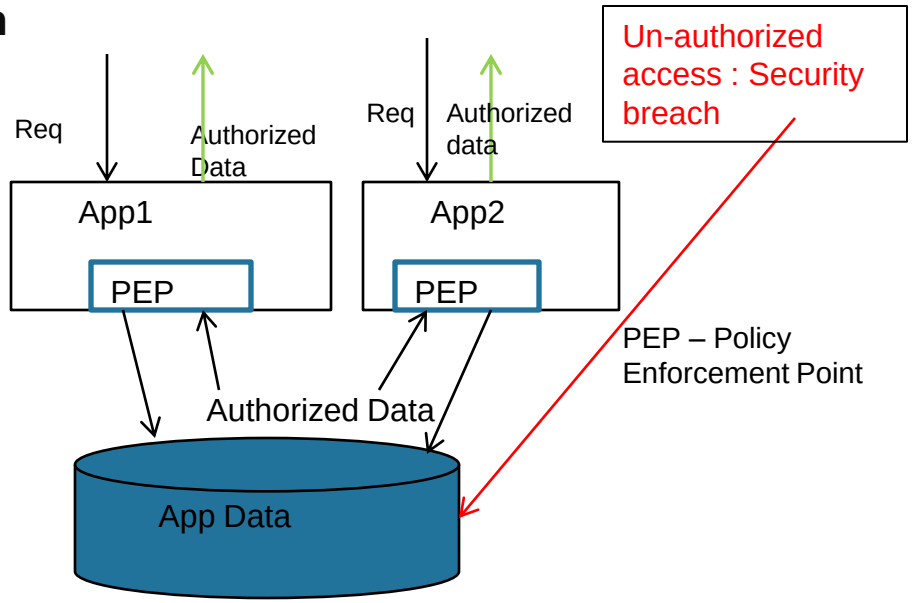
•Security is too tightly coupled with application code.

•If data is accessed by multiple applications, each application needs implement same or similar security and authorization logic.

•Security implementation may be embedded into each application, making code sharing difficult.

•Replacing application layer requires re-implementing data authorization.

•One can access un-authorized data by bypassing Application Layer, thus causing breach of security.



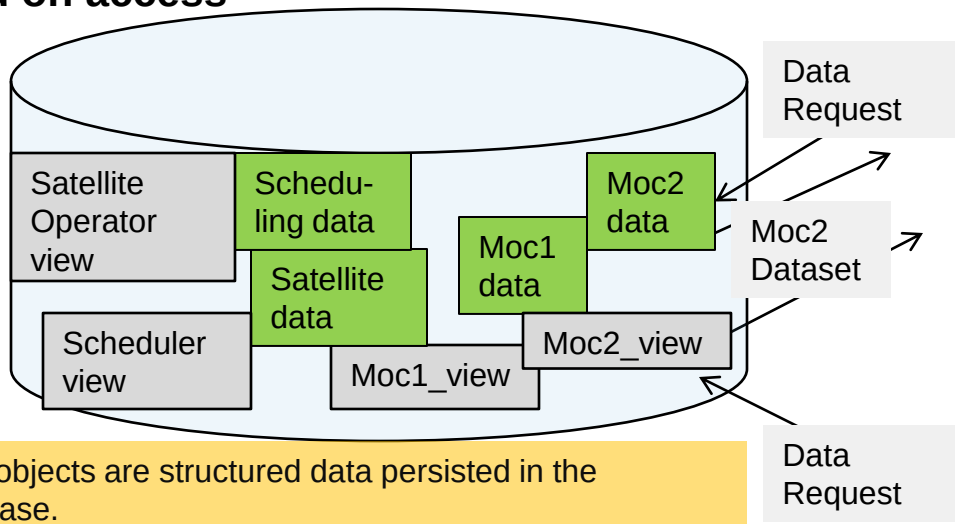
Existing Methods of Data Access Control (contd.)

At the Data Layer :

- **Creating separate storage views based on access**

Pro :

- *Access Decision is in the Data Layer.*
- *All data access application will have consistent view.*
- *Bypassing security is more difficult as Data authorization is integrated with the data storage/view.*



Data objects are structured data persisted in the database.
Views are result sets returned by a stored query in the database.

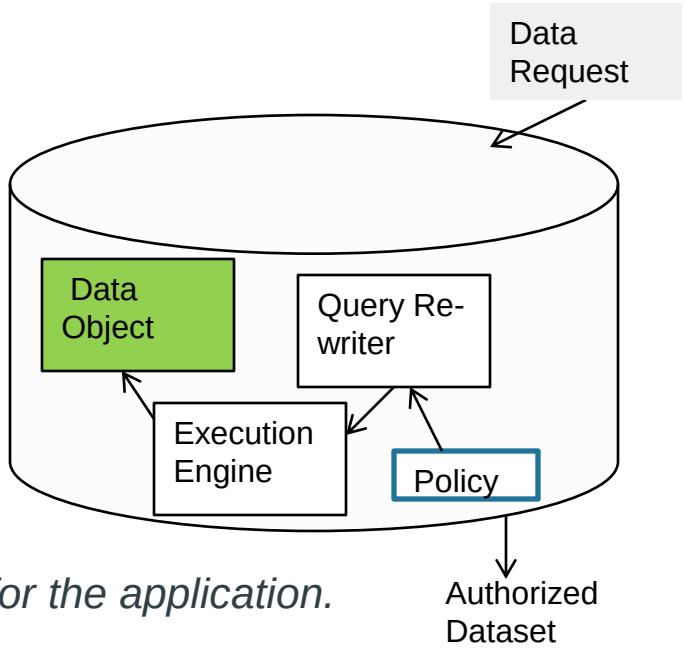
Con :

- *Designing data architecture based on access control can lead to duplicate data and/or redundant tables/views.*
- *Fine grained access can be difficult to define.*

Existing Methods of Data Access Control (contd.)

At the Data Layer :

- **Rewriting queries to return authorized set of data**



Pro :

- *Access Decision is in the Data Layer.*

  Dynamic query, based on the policy information persisted in the database, returns authorized dataset.
- *All data access applications have consistent view.*
- *Easy to replace Business Logic Layer without replacing Data Authorization Scheme.*
- *Policy definition or authorization rule can be specific for the application.*
- *Fine grained access of Data is possible.*
- *Data can be normalized to implement data validation, reduce storage redundancy and thus to improve data security.*

Con :

- *Careful design needs to be considered in order to keep performance impact to a minimum.*
-

Comparison of Data Authorization Schemes

Method	Architecture	Pro	Con
SQL Query re-write at Business Logic Layer	Business Logic Layer	•Fine Grain Access Permitted •Custom application need can be met. •Cost minimal – no dependence on external tool.	•Susceptible to sql injection attack. •Application layer security can be bypassed. •Not portable between applications. •Development cost involves developing custom code.
Application Framework Security	Business Logic Layer	•Fine Grain Access Permitted •Custom application need can be met. •Cost minimal – application framework cost involved. • Development requires framework configuration and less custom code	•Application layer security can be bypassed. •Not portable between applications.
Query re-write at Database using Oracle Virtual Private Database (VPD)	Data Layer	•Data security cannot be bypassed •Fine Grain Access Permitted •Custom application need can be met. •Cost minimal – VPD included in Oracle 11g license.	•Careful consideration needed for performance impact. •Development cost involves Security function design and implementation.
Query re-write at Database using Oracle Label Security	Data Layer	•Data security cannot be bypassed •Fine Grain Access Permitted •Custom application need can be met. •Configuration based. Less custom code involved	•License cost is involved. •For systems with few attributes, tool configuration may be “overkill”
Query re-write at Database using Oracle Entitlement Server.	Data Layer	•Data security cannot be bypassed •Fine Grain Access Permitted •Custom application need can be met. •Configuration based. Less custom code involved	•License cost is involved. •Server set up can be involved and time consuming.

Query Rewrite at Data Layer seems to provide best data privacy but some solution may require significant license cost based on the Database Vendor.

Limitations of Present Schemes

- **Classical Role Based Access Control (RBAC) alone cannot provide Space Ground System Fine Grained Data Authorization**
  - *Different MOC will have personnel with same role.*
  - *Ground System personnel can have different permissions for the same data object.*
- **Present schemes of Attribute Based Access Control (ABAC) does not fit into Space Ground System data security scheme without modification.**
  - *Present ABAC schemes depend on permission based on subject, resource or environmental attributes such as identity, location, date etc.*
  - *Ground System data access does not depend on data requester identity or security level.*
  - *Ground System data may depend on simple or complex attribute types.*
  - *Some, not all Ground System Data need Fine Grained access.*

Classical RBAC and ABAC schemes may be limited in defining Space Ground System Data Access Control efficiently.

Access Control for Multi-Mission Space Ground System Data

Our goal was to develop a Data Authorization Scheme that :

- Meets Space Ground System Functional Requirements.
  - *Apply Data Normalization for the data to avoid data redundancy and add data validation.*
  - *Access Control to support "need-to-know" principle.*
- Provides data security that is not easily compromised.
  - *Inclusion of Hardware that supports necessary security level.*
  - *Maintaining user credential and permission in one secure application.*
- Less dependent on Business Intelligence Layer .
- Centralized Administration Model of users, groups and attribute permission.
- Meets performance requirement of Space Ground System.
- Cost Effective.

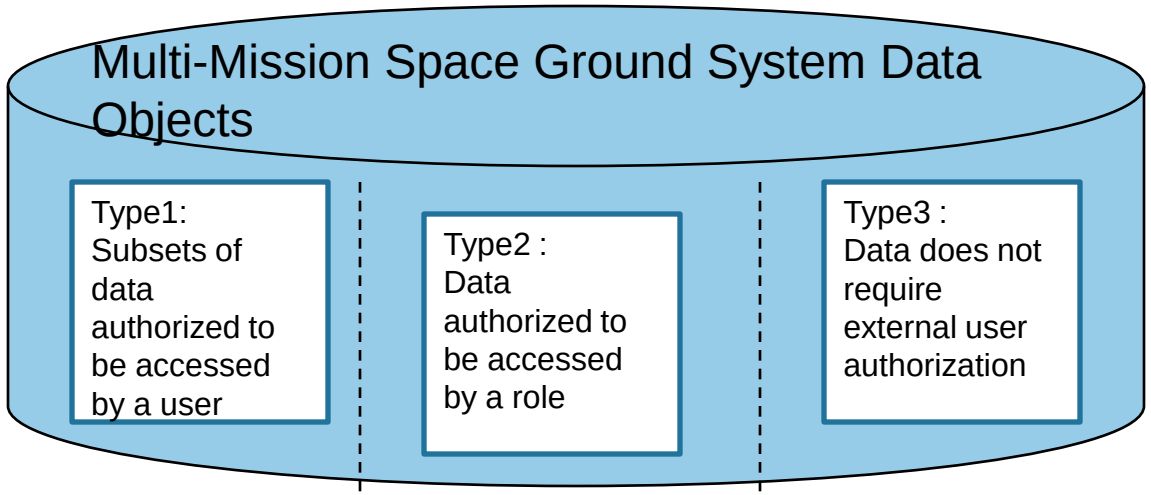
Attribute based Access Control for Multi-Mission Ground Systems (ABAC – MG)

Key Points of the Scheme :

- Permissions are pre-determined and are based on Mission and Space Ground System attributes rather than subject/resource attributes.
- Attributes can be complex based on Space Ground System Requirements and Data Architecture.
- Permission can be assigned and maintained per group of users instead of per single user while access is granted per user basis.
- One user can be assigned to only one group at one point of time.
- Permissions are maintained and controlled from one central repository along with the user credentials.
- Policy Enforcement Point (PEP) kept at the Data Layer using dynamic query re-write scheme at the Data Layer.
  - Oracle VPD has been used for query re-write implementation .
- Policy is defined taking Data Access performance into consideration.

Space Ground System Data Classification

Since Query Re-write impacts performance, data categorized to select authorization scheme.



Only Type 1 Data Requires Fine Grained Access and Query Re-write

Data Authorization requires ABAC-MG Fine Grained Access Policy.

MOC-1 …… MOC-N

Scheduler, Satellite Operator, .. …

RBAC is sufficient for Access Policy.

MOC

Scheduler

User credential is sufficient. No special Data Authorization Policy.

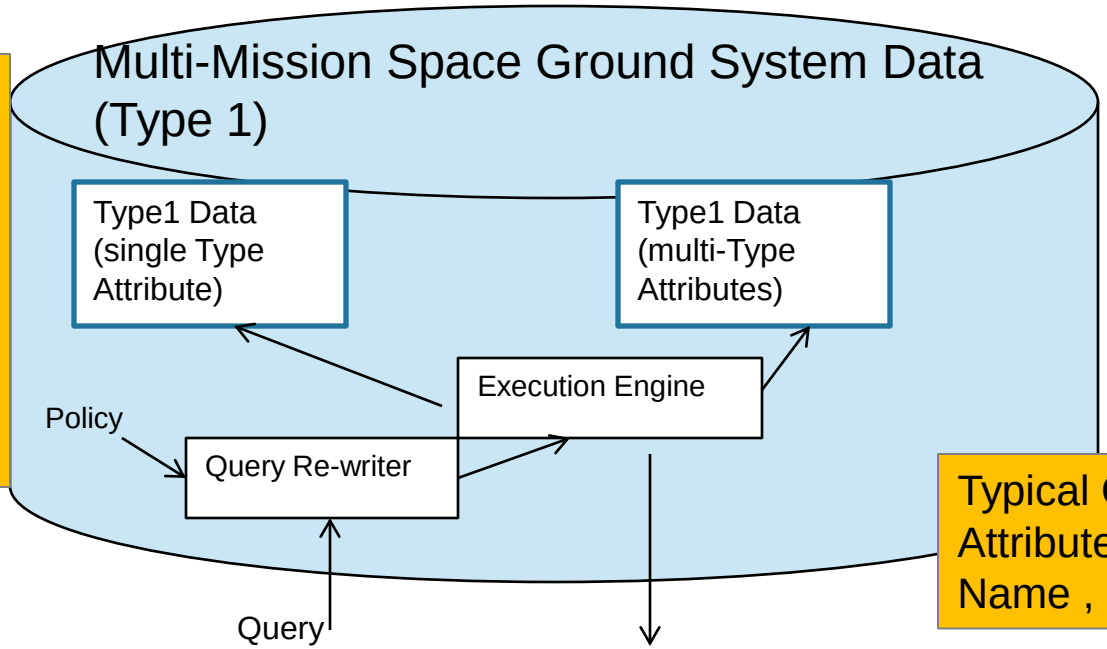
User 1…User N (with valid credential)

Careful categorization of Data reduces number of Query Re-writes and thus improves performance of Data Access.

Space Ground System Data Classification (contd.)

Type 1 data are data objects that depend on Mission and Ground System attributes that will have selective access.

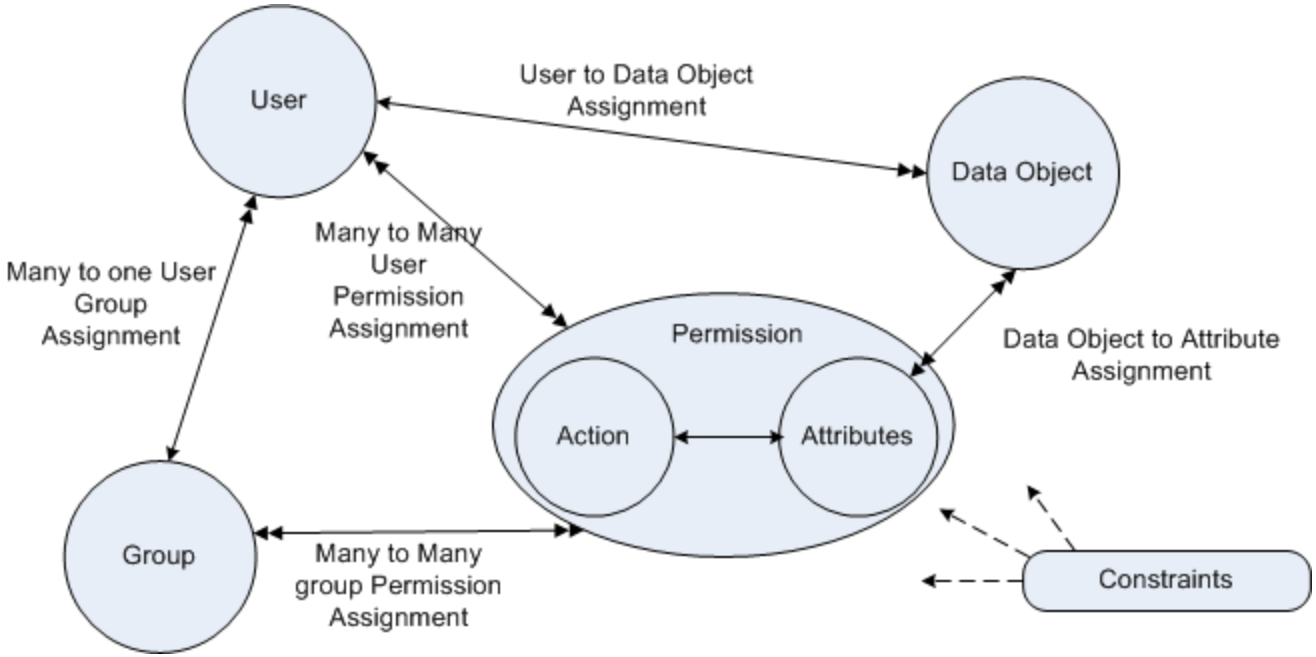
Data object can contain one or more unique type(s) of attribute(s) on which access permission is specified.



Typical Ground System Attributes are : Mission Name , service type etc.

ABAC-MG defines single Policy to access data with both single and multi-type attributes.

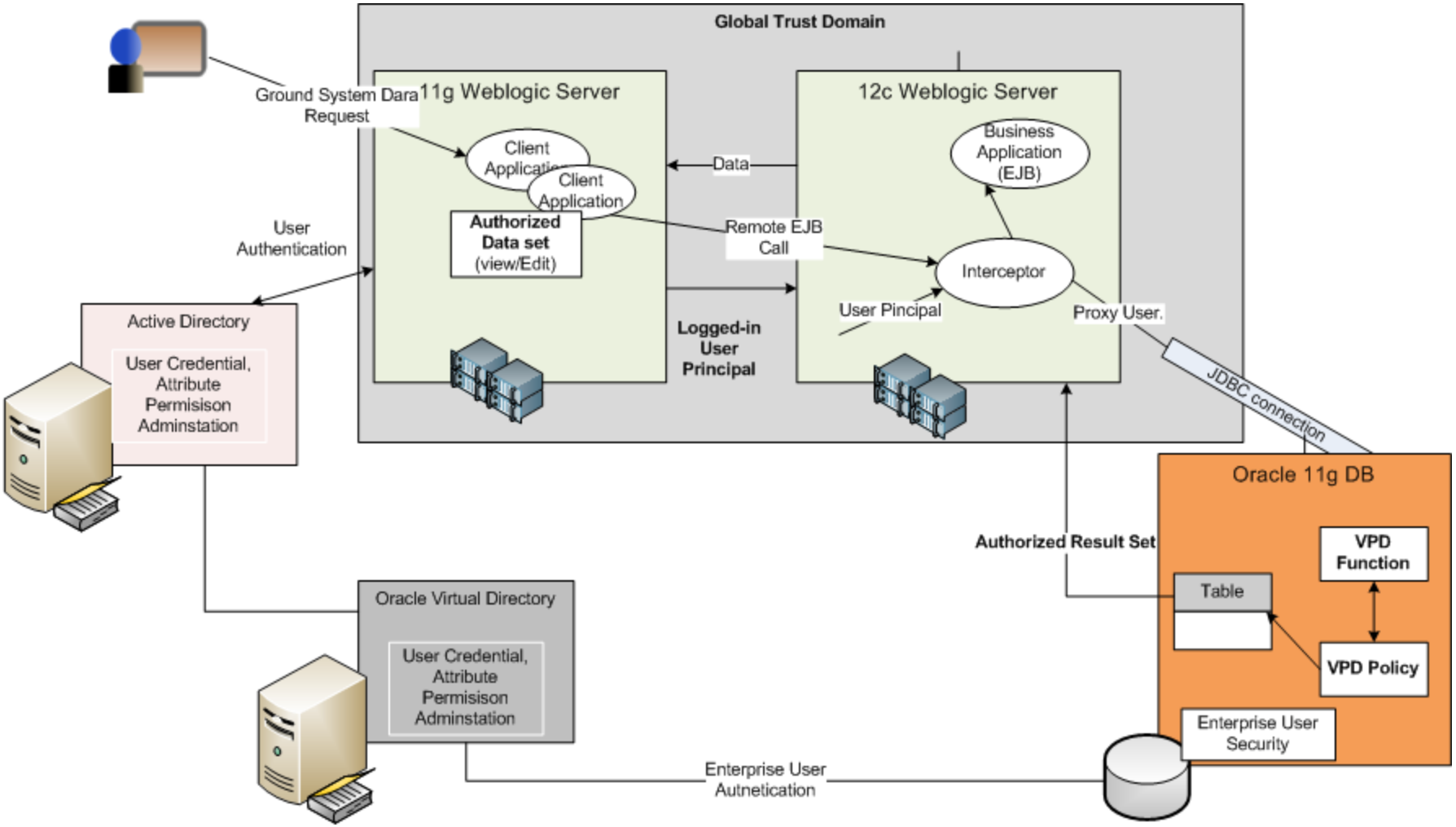
Components of ABAC-MG



Group – Set of Multi-Mission Ground System user groups, contains access permissions on Mission Ground system attributes.
User – Set of users assigned to a particular group.
Permission – Set of permission objects each defined as attribute and action on the attribute.
Attribute – Set of composite objects, each composed of type of the attribute and value.
Data Object - Set of Data objects contains single or multiple Space Ground attributes.
Constraints - set of authorization constraints enforced on different relations.

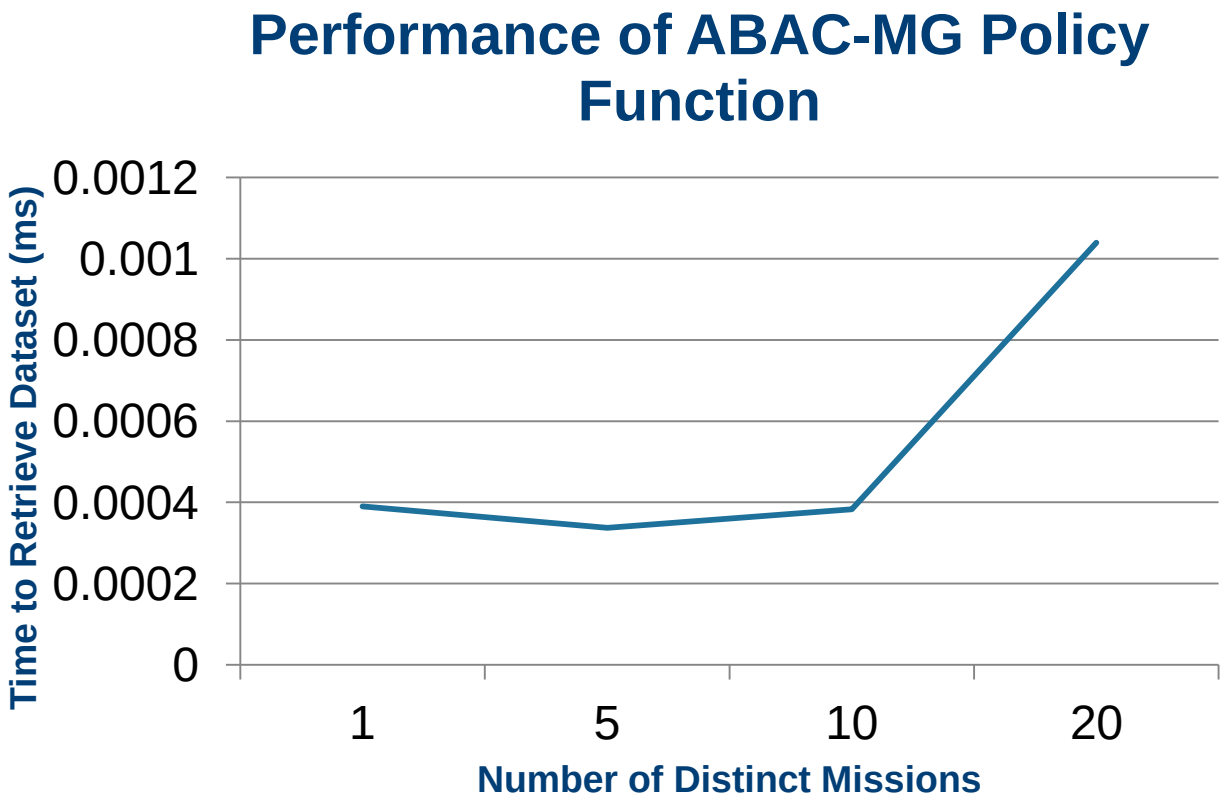
Permissions are specified on System Attributes, and can be assigned to groups.
Permissions, groups, users are managed in a central repository.

ABAC-MG Deployment Layout



Users are Enterprise Users, using a single pooled proxy connection, managed from a central location, outside of Application or Data Layer.

Performance of Data Access in ABAC-MG



Only Single Attribute Dependency is considered

Total Dataset size = 1700; Each data instance is for a Mission

Time to retrieve authorized dataset increases with number of missions in the system. In ABAC-MG time to retrieve dataset is ~ 1 microsec for a model system with 20 missions.

Summary

- Multi-Mission Ground System Data Access may require Fine Grained Access Control in some deployment scenario.
- Classical RBAC and/or ABAC may not fulfill Multi-Mission Ground System Data Authorization requirements completely.
- ABAC-MG provides a cost efficient scheme to provide robust data protection for Multi-Mission Ground System Data.
- By considering Separation of Duties (SOD) and applying Fine Grained Access Control selectively along with classical RBAC scheme, ABAC-MG provides a performance improved Data Authorization Scheme.
- Administration of authorization information is centralized and secure as users, groups and permissions are maintained along with user credentials.
- Performance analysis of ABAC-MG policy function is done based on single attribute dependent data. More analysis is needed for both single and multi-attribute data access.

Key References

1. Ravi S. Sandhu, Edward J. Coynek, Hal L. Feinsteink and Charles E. Youmank, *Role-Based Access Control Models*, IEEE Computer, Volume 29, Number 2, February 1996
2. Ravi Sandhu, Venkata Bhamidipati, Qamar Munawer, *The ARBAC97 Model for Role-Based Administration of Roles*, ACM Transactions on Information and System Security, Vol. 2, No. 1, February 1999.
3. Jaehong Park , Ravi Sandhu, *Towards Usage Control Models: Beyond Traditional Access Control (2002)*, In Proceedings of 7th ACM Symposium on Access Control Models and Technologies, 2002.
4. Yonghe Wei, Chunjing Shi, Weiping Shao, *An Attribute and Role based Access Control Model for Service-Oriented Environment*, Chinese Control and Decision Conference, 2010
5. E. Yuan and J. Tong, *Attributed Based Access Control (ABAC) for Web Services*, Proceedings of the IEEE International Conference on Web Services, 561-569, 2005.
6. Shen Hai-bo, Hong Fan, *An Attribute-Based Access Control Model for Web Services*, Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, 2006.
7. Alan H. Karp, Harry Haury, Michael H. Davis, *From ABAC to ZBAC: The Evolution of Access Control Models*, Tech. report HPL-2009-30, HP Labs, 21 Feb. 2009.
8. D. Richard. Kuhn, Edward J. Coyne, Timothy R. Weil, *Adding Attributes to Role-Based Access Control*, *IEEE Computer, vol. 43, no. 6 , 2010.*
9. Vincent Hu, Adam Schnitzer, Ken Sandlin, *Attribute Based Access Control Definition and Considerations*, NIST Special Publication 800-162.
10. S. Chaudhuri, R. Kaushik, R Ramamurthy, *Database Access Control & Privacy: Is There A Common Ground?,* In: Proceedings of CIDR 2011, 2011.