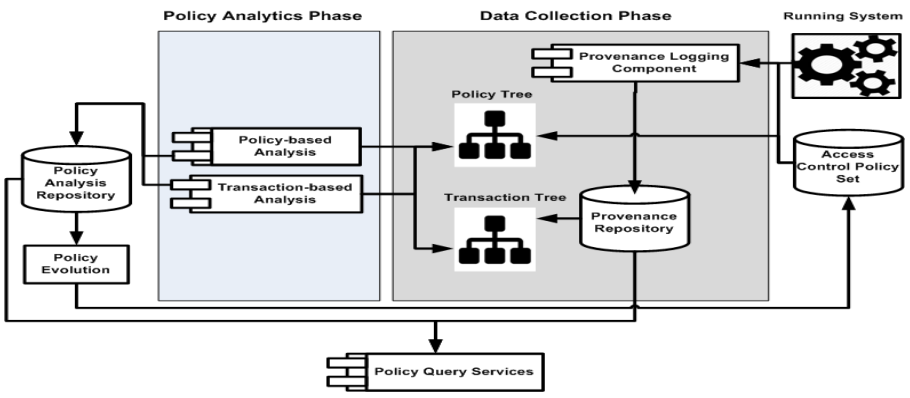
Provenance-based Analytics Services for Access Control Policies

Elisa Bertino (Purdue University), **Amani Abu Jabal** (Purdue University), **Seraphin Calo** (IBM), **Christian Makaya** (IBM), **Maroun Touma** (IBM), Dinesh Verma (IBM), Christopher Williams (DSTL)

Policy Quality Requirements

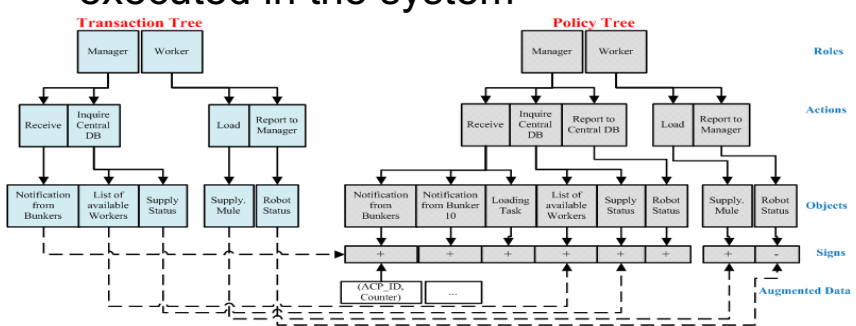
- Inconsistency: reduce conflict resolutions
- Policies Exceptions: determine if policies need to be modified to cover the frequently occurring exceptions.
- Incompleteness: enhance the predictability of device behaviors
- Redundancy: reduce the size of the policy set and enhances security.
- Irrelevancy: minimize exploitations

Proposed Framework



Policy Analysis Structures

- **Policy Tree:** multi-way tree represents the access control policies
- **Transaction Tree:** multi-way tree represents the transactions that are executed in the system



Policy Analytics Services

❖ Policy-based Analysis

Input: *PolicyTree*
1. Traverse each path in *PolicyTree* from the root (role node) to an object node
2. If a path branches to two different signs
3. Flag for inconsistency
4. If the leaf node of a path is augmented with multiple policy IDs
5. Flag for redundancy
6. If the counter value of a leaf node is zero
7. Flag for irrelevancy
8. Traverse each path in *PolicyTree* from the root (role node) to an action node
9. If there are object nodes which are composite of each other
10. Asses for inconsistency
11. Asses for redundancy

❖ Transaction-based Analysis

Input: *TransactionTree*, *PolicyTree*, *SimP*
1. Traverse each path in the *TransactionTree* and explores its corresponding policies in the *PolicyTree*
2. If a transaction path does not point to any policy
3. Flag for incompleteness
4. If a transaction points to two policies which have unequal sign
5. Flag for inconsistency
6. If a transaction points to one policy path but the path is augmented with multiple policy IDs
7. Flag for redundancy
8. If a transaction points to a policy path where the sign of the policy is '-'
9. Flag for exception

❖ Analytics objectives

	Policy-based Analysis	Transaction-based Analysis
Inconsistency	✓	✓
Exception	✘	✓
Incompleteness	✘	✓
Redundancy	✓	✓
Irrelevancy	✓	✘

Query Services

- Queries on the Quality of Policies: retrieve the policies which do not satisfy quality metrics.
- Queries on Policies: retrieve basic information on policies
- Queries on Transactions: retrieve information about the executed transactions
- Queries on Policy Analytics Statistics: retrieve aggregated analysis results

Conclusions

- Propose a set of metrics to evaluate the quality of access control policies
- Use provenance for capturing fine-grained metadata essential for evaluating the quality of policies
- Propose a framework which supports various types of services

Distributed Analytics and Information Science International Technology Alliance
Annual Fall Meeting, September 2017