CERIAS

Policy-Driven Control and Management of Data Integrity

Elisa Bertino[1], Yonglak Sohn[2], Ji-Won Byun[1]
{bertino, ysohn, byunj}@cs.purdue.edu
[1] CERIAS and Department of Computer Science, Purdue University
[2] Department of Computer Engineering, Seokyeong University

Integrity Requirements

1. Control of information flow
High integrity objects should not be contaminated by low integrity objects.

2. Data verification
Only verified data should be provided to critical transactions.

3. Prevention of fraud and error
Only legitimate data should be introduced to system.

4. Autonomous data validation
Integrity of data should be maintained or enhanced by system.

Challenges

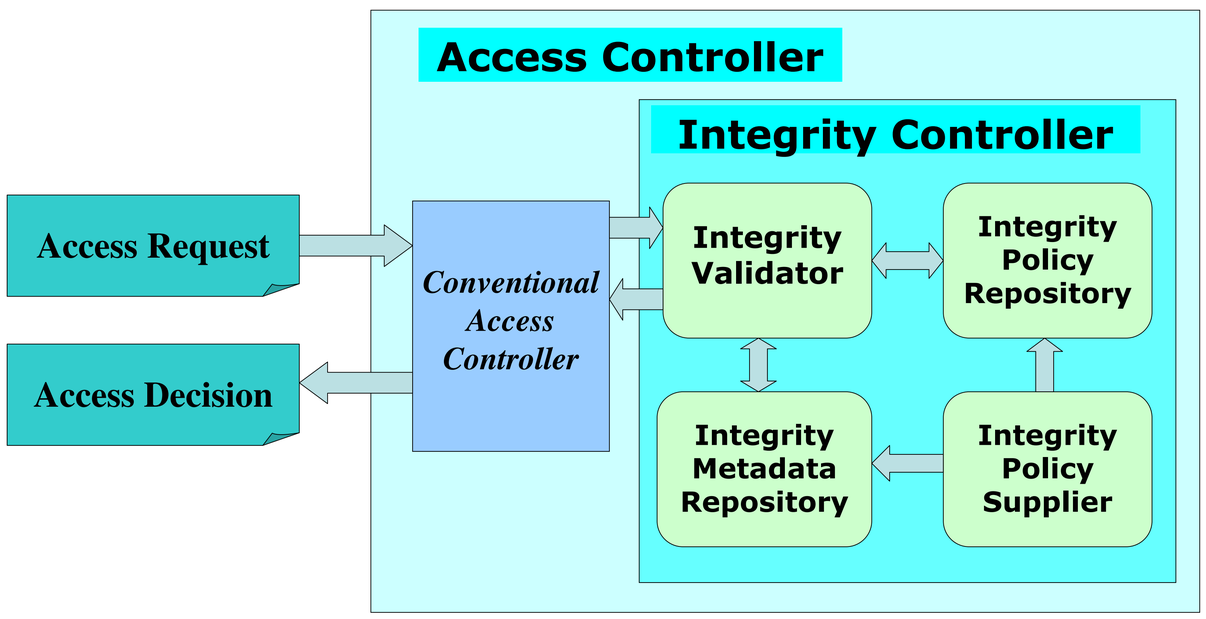
- √ *Each requirement calls for a different approach.*
- √ *Information system contains various types of data, each of which requires a different level of integrity.*
- √ *A comprehensive solution requires a systematic control of data access.*

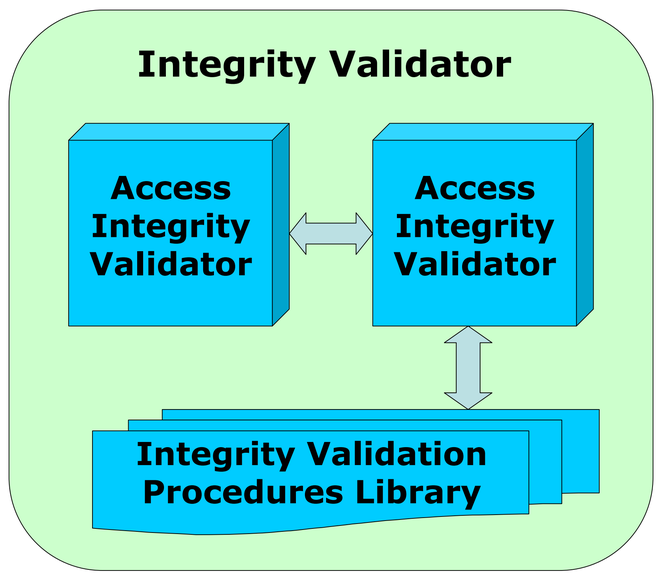
Our Solutions

1. Policy-driven control and management of data integrity.

2. Rich and flexible metadata to store detailed description of data.

3. Add-on control mechanism to existing access control.





Example Policies

```
DV-POLICY DVP-1 FOR AsD {
    WHEN ChangeOnData;
    IF revalidateAsD(this);
    THEN (AsD.validated ← true);
    ELSE (AsD.validated ← false);
}
```

When the ChangeOnData event occurs, AsD gets revalidated by the specified function. Whether or not the revalidation succeeds is reflected on the AsD.

```
AC-POLICY ACP-2 FOR (AsD, CL) {
    WHEN Read;
    IF (AsD.confidenceLevel ≥
                CL.preferredLevel);
    THEN Allow: ;
    ELSE Deny: writeToLog();
}
```

A CL can read an AsD item only if its confidence level is greater than or equal to his preference level. If an access is denied, the information about the denied access request should be recorded in the system log.

Current Achievements

- √ **Development of integrity policy specification languages**
- √ **Design of comprehensive integrity control system architecture**
- √ **Comparative study and analysis of existing integrity models**

Future Work

1. **Implementation on top of a real DBMS**
   : Evaluation of performance, scalability, and usability
2. **Refinement of policy specification language**
   : Investigation of expressiveness & completeness of current language
3. **Development of automatic data integrity enhancement/recovery**
   : Integration of policy-driven data cleansing techniques

PURDUE UNIVERSITY · PURDUE HOMELAND SECURITY INSTITUTE · CERIAS · REGENSTRIEF CENTER FOR HEALTHCARE ENGINEERING · Discovery Park e-Enterprise Center