

Mobile Policy-Based Guard

Amgad Fayad

703-983-6519 • afayad@mitre.org

Army MOIE

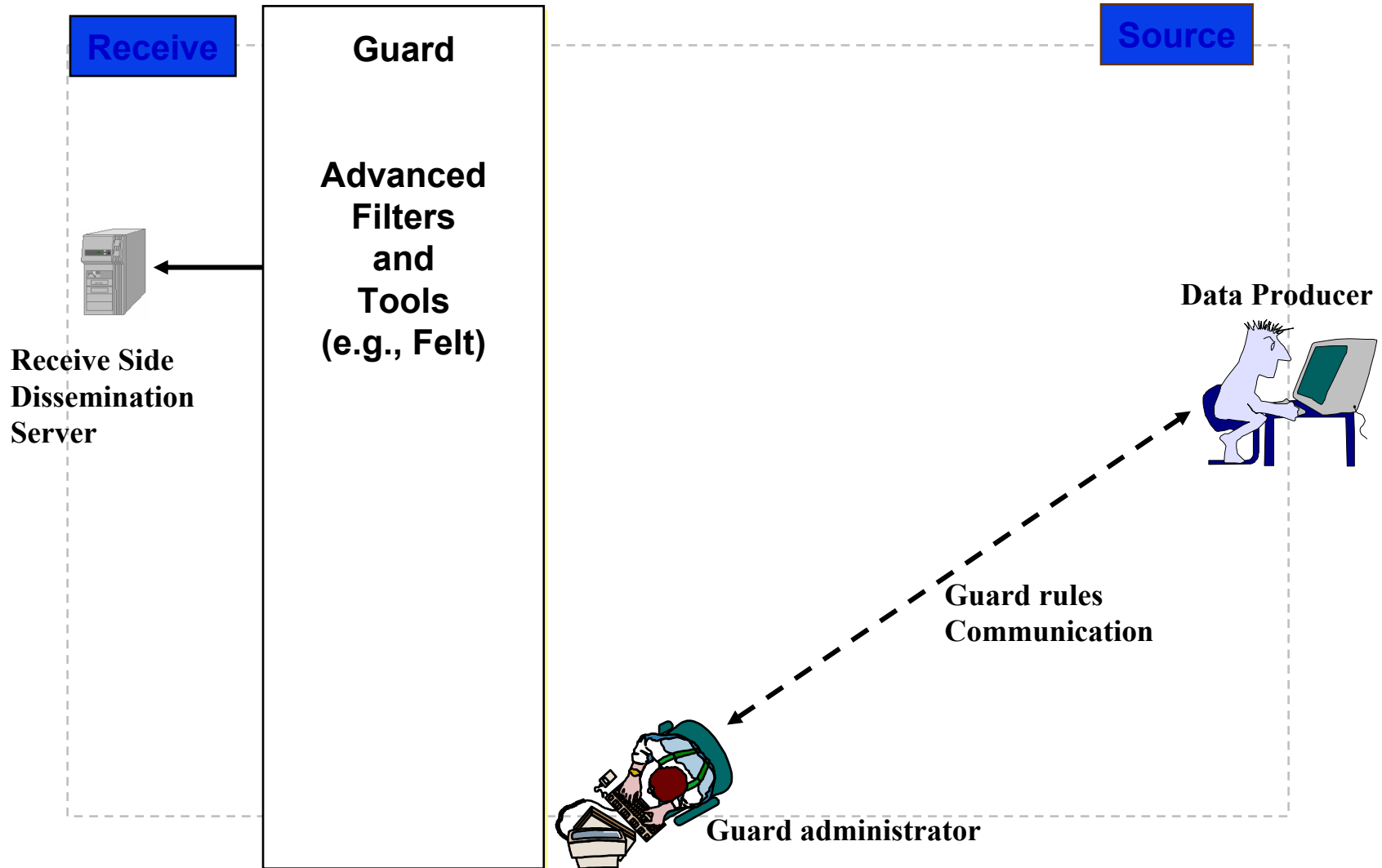
The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

Problem

- **Releasability rules are complex and depend on data types**
 - **Guard Data rules cannot be administered remotely**
 - **Guards are difficult to maintain and certify**
 - **Guards are inadequate for quick reaction coalition environments**
- **Once data is released through the guard, the source side has no method of control over access**

Background



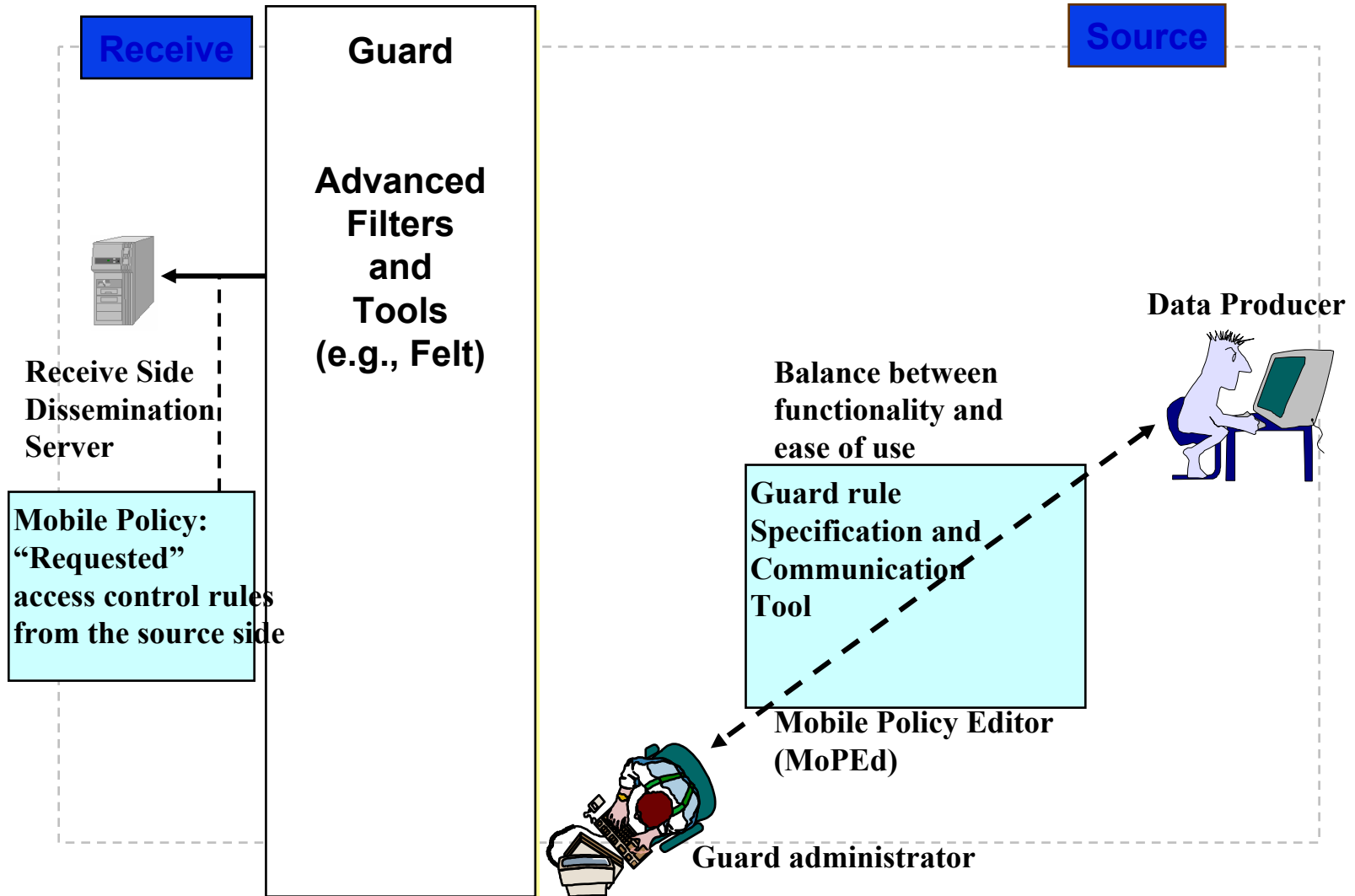
Objective

- **Improve guard maintainability**
- **Provide discretionary access control over data on the receiving side**
- **Make guards easier to administer and accredit**

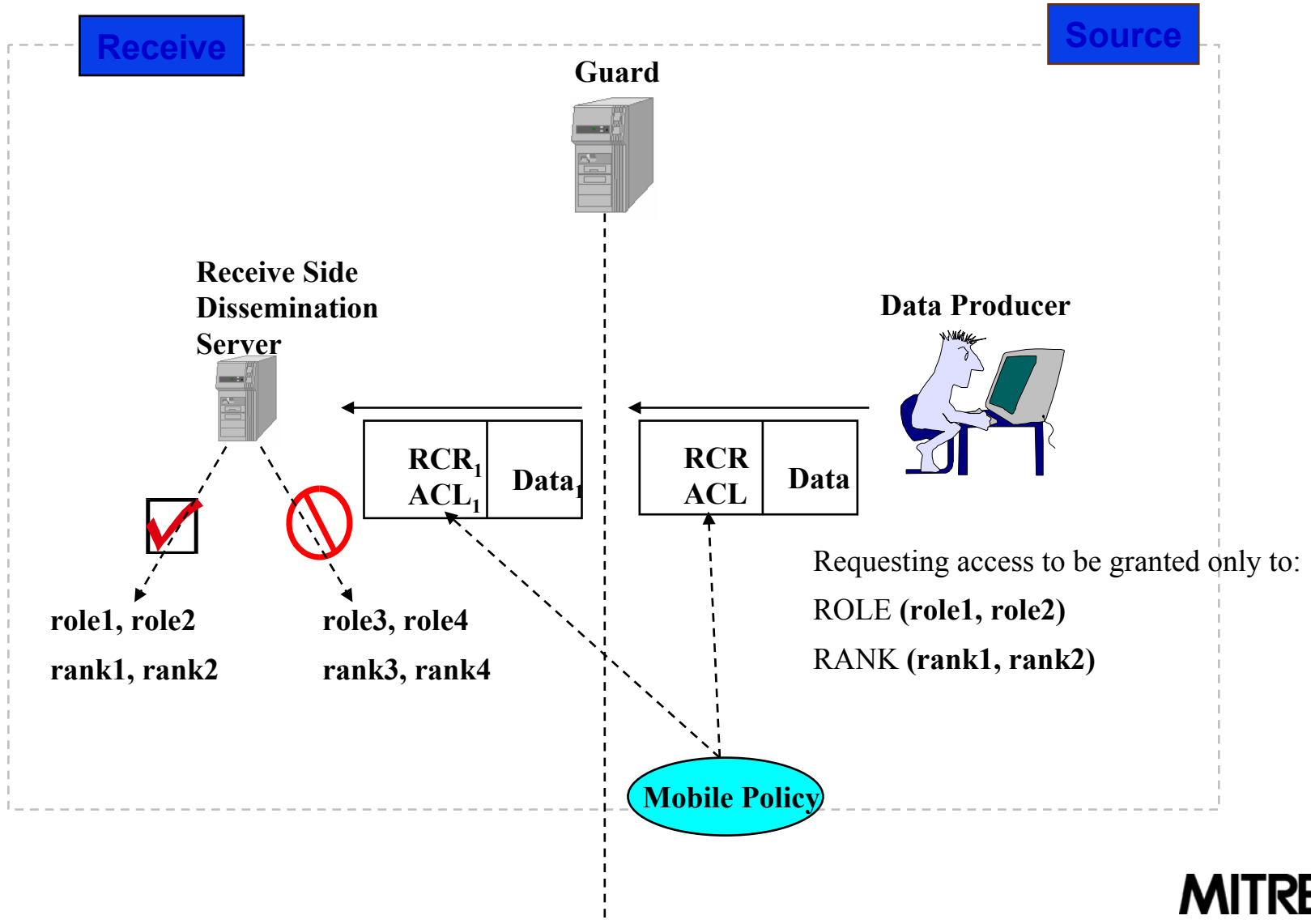
Activities

- **Analyze guard data and authority rule requirements**
- **Develop a release/access policy high-level language**
- **Develop a guard prototype using mobile policy and a Felt front-end**

Highlight



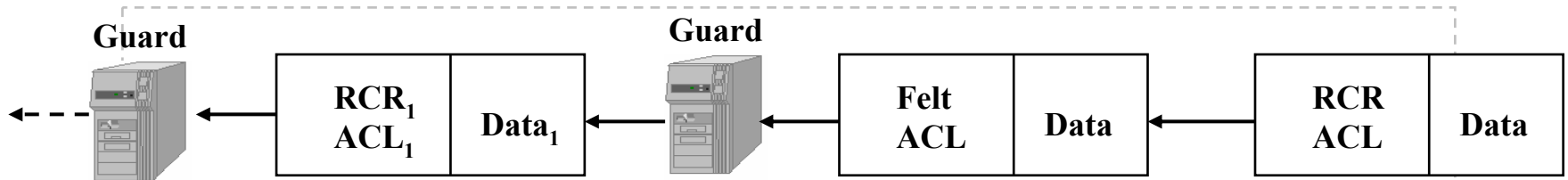
Highlight/Demonstration



Impacts

- **Provide a front-end to Felt for the ISSE and C2G Guards and ISC2 project**
 - **Looking for a balance between "human readability" and unambiguity in interpreting the rules**
- **Explore NIMA release control needs**
- **Explore possible impacts on the Defense Counterintelligence Information System (DCIIS) and the IC MAP project**

Future Plans



- Receive side can repeat the process if release through another guard is required

- ACL can be used to apply Discretionary Access Control (DAC) or Role-Based Access Control (RBAC)

- Source side data producer (owner) specifies Release Control Rules (RCR) and Access Control Rules (ACL) using MoPEd

- MoPEd uses the RCR as input and produces Felt code for the guard administrator to edit

- The guard filters the data and the ACL and produces filtered/sanitized data₁, new RCR₁ for another guard (optional), and sanitized ACL₁